

Số: 5 /BC-CATTT

Hà Nội, ngày 08 tháng 03 năm 2024

BÁO CÁO KỸ THUẬT

Tình hình an toàn thông tin tháng 02/2024 và thống kê kết nối chia sẻ dữ liệu về mã độc, giám sát

1. Cảnh báo an toàn thông tin đã phát hành trong tháng



Văn bản số 210/CATTT-NCSC về việc lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 02/2024 phát hàng ngày 22/02/2024.

2. Tình hình triển khai công tác phòng chống phần mềm độc hại và chia sẻ dữ liệu mã độc theo Chỉ thị 14/CT-TTg năm 2018

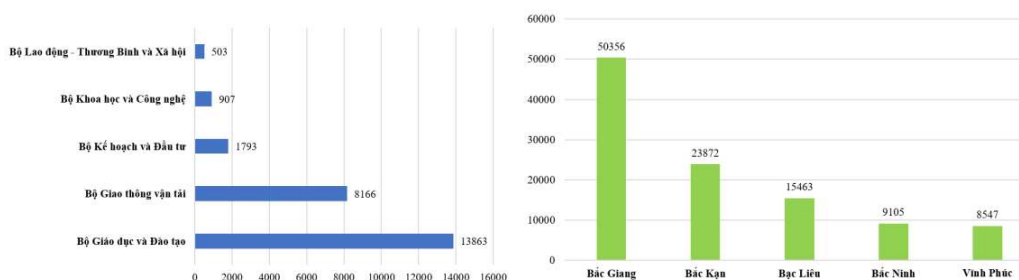
Thực hiện Chỉ thị số 14/CT-TTg của Thủ tướng Chính phủ ban hành ngày 25/5/2018 về việc nâng cao năng lực phòng, chống phần mềm độc hại, Cục An toàn thông tin đã giao Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC) hỗ trợ 15 doanh nghiệp có giải pháp phòng chống mã độc thực hiện kết nối chia sẻ dữ liệu mã độc theo văn bản 2290/BTTTT-CATTT ngày 17/7/2018 về việc hướng dẫn kết nối, chia sẻ thông tin về mã độc giữa các hệ thống kỹ thuật. Danh sách sản phẩm phòng chống mã độc có khả năng kết nối chia sẻ dữ liệu cập nhật tại: <https://ncsc.gov.vn/alert/danh-sach-san-pham-phong-chong-ma-oc-co-kha-nang-ket-noi-chia-se-du-lieu.81/>

Đến hết tháng 02/2024 đã có 88 đơn vị (63 Tỉnh/Thành, 25 Bộ/Ngành) triển khai giải pháp phòng chống mã độc tập trung và thực hiện kết nối chia sẻ thông tin về mã độc với Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC).

Trong tháng 02/2024, thông qua kết nối chia sẻ dữ liệu về mã độc từ 88 đơn vị, Hệ thống kỹ thuật của Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC) ghi nhận 79/88 đơn vị có kết nối thường xuyên. Trong các đơn vị kết nối thường xuyên có 79/80 đơn vị chia sẻ về hệ điều hành các máy (tổng số máy là 245.490).

Tính đến tháng 02/2024 có 03 đơn vị bao gồm: **Bộ Giáo dục và Đào tạo, Bộ Nông nghiệp và Phát triển nông thôn, Ủy ban Dân tộc** chưa thực hiện chia sẻ dữ liệu mã độc về Hệ thống kỹ thuật của Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC). Vì vậy, đề nghị các đơn vị thực hiện chia sẻ đầy đủ thông tin dữ liệu mã độc nhằm nâng cao năng lực phòng, chống phần mềm độc hại và thực hiện đánh giá chỉ số lây nhiễm phần mềm độc hại ở các bộ, ngành, địa phương, coi đây là một trong những tiêu chí đánh giá mức độ bảo đảm an toàn thông tin của các bộ, ngành, địa phương.

Một số đơn vị có số lượng máy chia sẻ trong tháng tương đối đầy đủ:



Ghi chú: Hiện trạng triển khai giải pháp phòng chống mã độc đáp ứng yêu cầu của Chỉ thị số 14/CT-TTg năm 2018 tại Phụ lục I kèm theo.

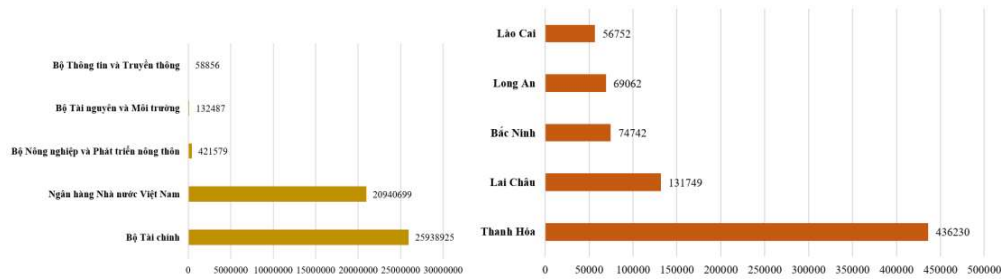
3. Tình hình triển khai công tác giám sát an toàn thông tin và kết nối chia sẻ dữ liệu giám sát theo Chỉ thị 14/CT-TTg năm 2019

Thực hiện Chỉ thị số 14/CT-TTg của Thủ tướng Chính phủ ban hành ngày 07/6/2019 về việc tăng cường bảo đảm an toàn, an ninh mạng nhằm cải thiện chỉ số xếp hạng của Việt Nam, Cục An toàn thông tin đã giao Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC) hỗ trợ 15 doanh nghiệp có giải pháp giám sát an toàn thông tin thực hiện kết nối chia sẻ dữ liệu theo văn bản 2973/BTTTT-CATTT ngày 04/9/2019 về việc hướng dẫn triển khai hoạt động giám sát an toàn thông tin trong cơ quan, tổ chức nhà nước. Danh sách nền tảng dịch vụ SOC đáp ứng yêu cầu kết nối, chia sẻ thông tin cập nhật tại: <https://khonggianmang.vn/alert/danh-sach-nen-tang-dich-vu-soc-ap-ung-yeu-cau-ket-noi-chia-se-thong-tin.150/>

Đến hết tháng 02/2024 đã có 87 đơn vị (63 Tỉnh/Thành, 24 Bộ/Ngành) triển khai công tác giám sát an toàn thông tin và thực hiện kết nối chia sẻ dữ liệu giám sát với Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC).

Trong tháng 02/2024, thông qua kết nối chia sẻ dữ liệu giám sát từ 87 đơn vị, Hệ thống kỹ thuật của Trung tâm Giám sát an toàn không gian mạng quốc gia ghi nhận 70/87 đơn vị có kết nối chia sẻ dữ liệu tương đối đầy đủ, 17/87 đơn vị bị mất kết nối chia sẻ dữ liệu.

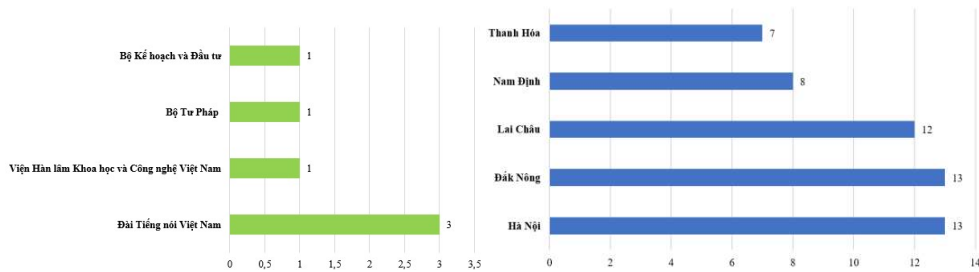
Một số đơn vị có kết nối chia sẻ dữ liệu giám sát trong tháng tương đối đầy đủ:



Ghi chú: Hiện trạng kết nối chia sẻ dữ liệu giám sát tại Phụ lục II kèm theo.

4. Tình hình lây nhiễm mã độc trên cả nước

Trong tháng, Hệ thống kỹ thuật của Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC) đã ghi nhận **364.369** địa chỉ IP của Việt Nam nằm trong mạng botnet (giảm 32.78% so với tháng 01/2024), trong đó có 95 địa chỉ IP của cơ quan, tổ chức nhà nước (6 địa chỉ IP Bộ/Ngành, 89 địa chỉ IP Tỉnh/Thành).



Ghi chú: Danh sách các đơn vị có địa chỉ IP nằm trong mạng botnet Trung tâm NCSC phát hiện có tại Phụ lục III kèm theo.

Thông tin chi tiết về các địa chỉ IP nằm trong mạng botnet đơn vị chuyên trách về CNTT/ATTT tại Bộ/Ngành, Tỉnh/Thành có thể tra cứu, cập nhật thông tin thường xuyên thông qua tài khoản đã có trên Hệ thống giám sát từ xa do Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC) cấp. Thông tin từ Hệ thống cũng có thể tham khảo, sử dụng để đánh giá hiệu quả giải pháp giám sát, phòng chống mã độc tập trung đang triển khai.

5. Tình hình triển khai công tác dán nhãn Tín nhiệm mạng cho các trang, cổng thông tin điện tử theo Quyết định số 17/QĐ-UBQGCS năm 2023

Thực hiện nhiệm vụ được giao tại Quyết định số 964/QĐ-TTg ngày 10/8/2022 của Thủ tướng Chính phủ về phê duyệt chiến lược An toàn, An ninh mạng quốc gia, chủ động ứng phó với các thách thức từ không gian mạng đến

năm 2025, tầm nhìn 2023.

Thực hiện mục tiêu theo điểm h mục I.1 tại Quyết định số 17/QĐ-UBQGCDŞ ngày 04/4/2023 của Ủy ban Quốc gia về Chuyển đổi số về việc Ban hành Kế hoạch hoạt động của Ủy ban Quốc gia về chuyển đổi số năm 2023, các hoạt động đã triển khai để thực hiện mục tiêu “100% các trang, cổng thông tin điện tử của cơ quan nhà nước được đánh giá an toàn thông tin và dán nhãn tín nhiệm mạng”.

Đến hết tháng 02/2024 đã có **82** đơn vị (61 Tỉnh/Thành, 21 Bộ/Ngành) triển khai công tác dán nhãn Tín nhiệm mạng cho các trang, cổng thông tin điện tử. Tổng số trang, cổng thông tin điện tử của các đơn vị cơ quan nhà nước đã được cấp nhãn Tín nhiệm mạng 4.678 website (557 website của 21 Bộ/Ngành, 4121 website của 61 Tỉnh/Thành).

Ghi chú: Hiện trạng triển khai công tác dán nhãn Tín nhiệm mạng theo Quyết định số 17/QĐ-UBQGCDŞ năm 2023 tại Phụ lục IV kèm theo.

6. Điểm yếu, lỗ hổng tồn tại trên máy tính của các cơ quan tổ chức

Trong tháng, Hệ thống kỹ thuật của NCSC đã ghi nhận có **76.507** điểm yếu, lỗ hổng an toàn thông tin tại các hệ thống thông tin của các cơ quan tổ chức nhà nước. Số lượng điểm yếu, lỗ hổng nêu trên là rất lớn, do đó Cục ATTT đã chỉ đạo Trung tâm Giám sát an toàn không gian mạng quốc gia triển khai đánh giá, xác định các lỗ hổng nguy hiểm, có ảnh hưởng trên diện rộng và hướng dẫn các Bộ/Ngành khắc phục. Đặc biệt có một số lỗ hổng đã và đang được các nhóm tấn công lợi dụng để thực hiện các cuộc tấn công APT. Dưới đây là một số lỗ hổng vẫn còn tồn tại trên nhiều máy chưa được xử lý.

TT	Mã điểm yếu/ lỗ hổng	SL máy bị ảnh hưởng	Ghi chú
1	CVE-2022-26809	18411	https://nvd.nist.gov/vuln/detail/CVE-2022-26809
2	CVE-2024-0814	9905	https://nvd.nist.gov/vuln/detail/CVE-2024-0814
3	CVE-2023-21716	8406	https://nvd.nist.gov/vuln/detail/CVE-2023-21716

4	CVE-2024-0519	8301	https://nvd.nist.gov/vuln/detail/ CVE-2024-0519
5	CVE-2022-35737	5040	https://nvd.nist.gov/vuln/detail/ CVE-2022-35737

Bên cạnh các điểm yếu/lỗ hổng ghi nhận, Hệ thống kỹ thuật của NCSC còn phân tích và phát hiện nhiều máy tính của cơ quan nhà nước có kết nối đến địa chỉ IP/Domain nghi ngờ độc hại do các phần mềm phòng chống mã độc đã ghi nhận. Thống kê TOP 6 kết nối nghi ngờ phát sinh trong tháng:

STT	IP/Domain nghi ngờ	IP/Domain nghi ngờ
1	cdn[.]specialtaskevents[.]com	ak[.]feethach[.]com
2	near[.]flyspecialline[.]com	four[.]startperfectsolutions[.]com
3	aitsath[.]com	epicunitscan[.]info

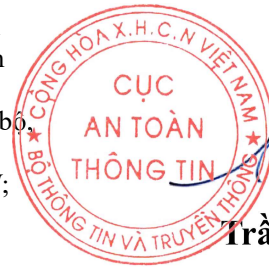
Nhằm đảm bảo an toàn hệ thống thông tin, đề nghị đơn vị chuyên trách về CNTT/ATTT tại cơ quan, tổ chức phối hợp với các đơn vị rà soát xác định và tiến hành “vá” các lỗi trên hệ thống, đặc biệt là các lỗ hổng nêu trên.

Trân trọng./.

Nơi nhận:

- Thứ trưởng Phạm Đức Long (để b/c);
- Đơn vị chuyên trách về ATTT/CNTT của Văn phòng Trung ương Đảng, Văn phòng Quốc hội, Văn phòng Chủ tịch nước, Tòa án Nhân dân tối cao, Viện Kiểm sát nhân dân tối cao, Kiểm toán Nhà nước;
- Đơn vị chuyên trách về ATTT/CNTT của các bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ;
- Sở TT&TT các tỉnh, thành phố trực thuộc TW;
- Các Cục: Viễn thông; Bưu điện Trung ương;
- Các Trung tâm: TTTT, VNNIC;
- Cục trưởng (để b/c);
- Các Phó Cục trưởng;
- Các phòng: ATHTTT, TT&HTQT;
- Trung tâm VNCERT/CC;
- Lưu: VT, NCSC.LTQ.

**KT. CỤC TRƯỞNG
PHÓ CỤC TRƯỞNG**



Trần Đăng Khoa

Phụ lục I

**TÌNH HÌNH TRIỂN KHAI GIẢI PHÁP PHÒNG CHỐNG
MÃ ĐỘC ĐÁP ỨNG YÊU CẦU CỦA CHỈ THỊ SỐ 14/CT-TTG NĂM 2018**
(Kèm theo Báo cáo số /BC-CATTT ngày tháng năm 2024
của Cục An toàn thông tin)

1. Danh sách Bộ/Ngành

TT	Bộ/Cơ quan ngang Bộ/ Cơ quan trực thuộc Chính phủ	Số lượng máy chia sẻ dữ liệu trong tháng 02/2024	Ghi chú
1	Bộ Công Thương	94	
2	Bộ Giáo dục và Đào tạo	0	Chưa chia sẻ
3	Bộ Giao thông vận tải	36	
4	Bộ Kế hoạch và Đầu tư	907	
5	Bộ Khoa học và Công nghệ	503	
6	Bộ Lao động - Thương Binh và Xã hội	0	Mất kết nối 01 tháng trở lên
7	Bộ Ngoại giao	7	
8	Bộ Nội vụ	65	
9	Bộ Nông nghiệp và Phát triển nông thôn	0	Chưa chia sẻ
10	Bộ Tài chính	151	
11	Bộ Tài nguyên và Môi trường	68	
12	Bộ Thông tin và Truyền thông	194	
13	Bộ Tư pháp	8166	
14	Bộ Văn hóa, Thể thao và Du lịch	22	
15	Bộ Xây Dựng	27	

16	Bộ Y tế	65	
17	Ngân hàng Nhà nước Việt Nam	1793	
18	Thanh tra Chính phủ	41	
19	Ủy ban Dân tộc	0	Chưa chia sẻ
20	Văn phòng Chính phủ	0	Mất kết nối 01 tháng trở lên
21	Ban Quản lý Lăng Chủ tịch Hồ Chí Minh	0	Mất kết nối 01 tháng trở lên
22	Bảo Hiểm Xã Hội	13863	
23	Đài tiếng nói Việt Nam	19	
24	Đài Truyền hình Việt Nam	348	
25	Thông tấn xã Việt Nam	0	Mất kết nối 01 tháng trở lên
26	Viện Hàn Lâm KHCN	137	
27	Viện Hàn Lâm KHXXH	188	
28	Kiểm toán Nhà nước Việt Nam	488	

2. Danh sách Tỉnh/Thành

TT	Tỉnh/Thành	Số lượng máy chia sẻ dữ liệu trong tháng 02/2024	Ghi chú
1	An Giang	498	
2	Bắc Giang	2922	
3	Bắc Kạn	3618	
4	Bạc Liêu	0	Mất kết nối 01 tháng trở lên
5	Bắc Ninh	1596	
6	Bà Rịa - Vũng Tàu	7815	
7	Bến Tre	33	
8	Bình Định	1	
9	Bình Dương	1	
10	Bình Phước	3603	
11	Bình Thuận	3015	
12	Cà Mau	15463	
13	Cần Thơ	2270	
14	Cao Bằng	1828	
15	Đắk Lắk	5200	
16	Đắk Nông	1322	

17	Đà Nẵng	23872	
18	Điện Biên	3715	
19	Đồng Nai	2633	
20	Đồng Tháp	8114	
21	Gia Lai	20	
22	Hà Giang	6	
23	Hải Dương	4088	
24	Hải Phòng	17	
25	Hà Nam	865	
26	Hà Nội	159	
27	Hà Tĩnh	2303	
28	Hòa Bình	0	Mất kết nối 01 tháng trở lên
29	Hồ Chí Minh	8080	
30	Hậu Giang	968	
31	Hưng Yên	384	
32	Khánh Hòa	2574	
33	Kiên Giang	6082	
34	Kon Tum	3396	

35	Lai Châu	28	
36	Lâm Đồng	2476	
37	Lạng Sơn	286	
38	Lào Cai	3	
39	Long An	2735	
40	Nam Định	43	
41	Nghệ An	5128	
42	Ninh Bình	0	Mất kết nối 01 tháng trở lên
43	Ninh Thuận	869	
44	Phú Thọ	12	
45	Phú Yên	39	
46	Quảng Bình	0	Mất kết nối 01 tháng trở lên
47	Quảng Nam	240	
48	Quảng Ngãi	3783	
49	Quảng Ninh	0	Mất kết nối 01 tháng trở lên
50	Quảng Trị	269	
51	Sóc Trăng	38	
52	Sơn La	4109	

53	Tây Ninh	1317	
54	Thái Bình	3870	
55	Thái Nguyên	2016	
56	Thanh Hóa	1164	
57	Thừa Thiên Huế	5486	
58	Tiền Giang	50356	
59	Trà Vinh	1177	
60	Tuyên Quang	3347	
61	Vĩnh Long	2875	
62	Vĩnh Phúc	9105	
63	Yên Bái	1076	

Ghi chú:

- Số lượng máy của mỗi đơn vị được tính dựa trên số lượng máy chia sẻ thông tin về hệ điều hành (trường “OS” trong văn bản 2290/BTTTT-CATTT ngày 17/7/2018 về việc hướng dẫn kết nối, chia sẻ thông tin về mã độc giữa các hệ thống kỹ thuật phát hành).

Phụ lục IV**TÌNH HÌNH TRIỂN KHAI DÁN NHÃN TÍN NHIỆM MẠNG TRÊN CÁC TRANG, CÔNG THÔNG TIN ĐIỆN TỬ CỦA CƠ QUAN NHÀ NƯỚC**

(Kèm theo Báo cáo số /BC-CATTT ngày tháng năm 2024
của Cục An toàn thông tin)

1. Danh sách Bộ/Ngành

TT	Bộ/Cơ quan ngang Bộ/ Cơ quan trực thuộc Chính phủ	Số lượng website được cấp nhãn đến tháng 02/2024	Số lượng website chưa thực hiện gắn nhãn đến tháng 02/2024	Ghi chú
1	Bộ Ngoại giao	96	9	
2	Bộ Nội vụ	10	6	
3	Bộ Tư pháp	55	6	
4	Bộ Kế hoạch và Đầu tư	1	0	
5	Bộ Tài chính	135	4	
6	Bộ Công Thương	13	3	
7	Bộ Nông nghiệp và Phát triển nông thôn	11	4	
8	Bộ Giao thông vận tải	6	2	
9	Bộ Xây dựng	0	0	Chưa đăng ký
10	Bộ Tài nguyên và Môi trường	0	0	Chưa đăng ký
11	Bộ Thông tin và Truyền thông	16	4	
12	Bộ Lao động - Thương binh và Xã hội	1	0	
13	Bộ Văn hóa, Thể thao và Du lịch	1	0	
14	Bộ Khoa học và Công nghệ	19	0	
15	Bộ Giáo dục và Đào tạo	7	2	

16	Bộ Y tế	11	1	
17	Ủy ban Dân tộc	0	0	Chưa đăng ký
18	Ngân hàng Nhà nước Việt Nam	6	0	
19	Thanh tra Chính phủ	0	0	Chưa đăng ký
20	Văn phòng Chính phủ	1	1	
21	Đài Tiếng nói Việt Nam	0	0	Chưa đăng ký
22	Ban Quản lý Lăng Chủ tịch Hồ Chí Minh	2	0	
23	Bảo hiểm Xã hội Việt Nam	75	2	
24	Thông tấn xã Việt Nam	0	0	Chưa đăng ký
25	Đài Truyền hình Việt Nam	1	0	
26	Viện Hàn lâm Khoa học và Công nghệ Việt Nam	0	0	Chưa đăng ký
27	Viện Hàn lâm Khoa học Xã hội Việt Nam	6	2	
28	Ủy ban quản lý vốn nhà nước tại doanh nghiệp	0	0	Chưa đăng ký
29	Tòa Án nhân dân tối cao	84	1	

2. Danh sách Tỉnh/Thành

TT	Tỉnh/Thành	Số lượng website được cấp nhãn đến tháng 02/2024	Số lượng website chưa thực hiện gán nhãn đến tháng 02/2024	Ghi chú
1	An Giang	202	0	
2	Bà Rịa – Vũng Tàu	124	15	
3	Bắc Giang	37	0	
4	Bắc Kạn	49	8	
5	Bạc Liêu	5	0	
6	Bắc Ninh	64	0	
7	Bến Tre	36	2	
8	Bình Định	35	8	
9	Bình Dương	30	11	
10	Bình Phước	44	19	
11	Bình Thuận	73	13	
12	Cà Mau	43	0	
13	Cần Thơ	20	0	
14	Cao Bằng	201	0	
15	Đà Nẵng	123	24	

16	Đắk Lắk	6	4	
17	Đắk Nông	27	3	
18	Điện Biên	40	10	
19	Đồng Nai	43	1	
20	Đồng Tháp	70	18	
21	Gia Lai	78	17	
22	Hà Giang	0	0	Chưa đăng ký
23	Hà Nam	28	24	
24	Hà Nội	280	126	
25	Hà Tĩnh	0	0	Chưa đăng ký
26	Hải Dương	14	3	
27	Hải Phòng	18	0	
28	Hậu Giang	33	14	
29	Hòa Bình	168	2	
30	Hưng Yên	30	30	
31	Khánh Hòa	178	15	
32	Kiên Giang	70	8	
33	Kon Tum	16	6	

34	Lai Châu	3	1	
35	Lâm Đồng	61	1	
36	Lạng Sơn	4	2	
37	Lào Cai	56	0	
38	Long An	47	0	
39	Nam Định	243	3	
40	Nghệ An	7	2	
41	Ninh Bình	24	0	
42	Ninh Thuận	30	0	
43	Phú Thọ	40	5	
44	Phú Yên	1	0	
45	Quảng Bình	33	12	
46	Quảng Nam	2	1	
47	Quảng Ngãi	254	10	
48	Quảng Ninh	28	2	
49	Quảng Trị	1	1	
50	Sóc Trăng	65	0	
51	Son La	39	2	

52	Tây Ninh	45	4	
53	Thái Bình	26	0	
54	Thái Nguyên	1	0	
55	Thanh Hóa	175	8	
56	Thừa Thiên Huế	285	69	
57	Tiền Giang	34	1	
58	TP Hồ Chí Minh	75	17	
59	Trà Vinh	92	30	
60	Tuyên Quang	8	2	
61	Vĩnh Long	168	10	
62	Vĩnh Phúc	52	8	
63	Yên Bái	37	13	