

Số: **01** /BC-CATT

Hà Nội, ngày **06** tháng **01** năm 2021

BÁO CÁO KỸ THUẬT

**Tình hình an toàn thông tin tháng 12/2021
và thống kê kết nối chia sẻ thông tin về mã độc**

1. Thông tin cảnh báo về các lỗ hổng bảo mật trong tháng

Cảnh báo số 5232/BTTTT-CATT ngày 21/12/2021 về việc rà soát, xử lý lỗ hổng Log4Shell gây ảnh hưởng nghiêm trọng trên diện rộng.

Cảnh báo số 1730/CATT-NCSC ngày 09/12/2021 về việc lỗ hổng bảo mật CVE-2021-41024 trong FortiOS và FortiProxy.

Cảnh báo số 1749/CATT-NCSC ngày 15/12/2021 về việc lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 12/2021.

Cảnh báo ngày 14/12/2021 về lỗ hổng bảo mật CVE-2021-4102 trong Google Chrome đang bị khai thác trong thực tế (qua email, page FB)

Cảnh báo số 1734/ CATT-NCSC ngày 10/12/2021 về việc lỗ hổng bảo mật ảnh hưởng nghiêm trọng trong Apache Log4j.

Cảnh báo ngày 08/12/2021 về lỗ hổng CVE-2021-43798 trên Grafana (qua email, page FB).

Cảnh báo ngày 15/12/2021 về 02 lỗ hổng (CVE-2021-42278, CVE-2021-42287) trong Active Directory (qua email. Page FB)

Nhằm hỗ trợ kịp thời các đơn vị trong công tác đảm bảo an toàn thông tin, bên cạnh hoạt động dự báo cũng như cảnh báo về điểm yếu, lỗ hổng và nguy cơ tấn công mạng, Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC), Cục An toàn thông tin tiếp tục theo dõi, cảnh báo đến các cơ quan tổ chức thông qua hệ thống các đơn vị chuyên trách về CNTT/ATTT khi phát hiện đã có tấn công vào hệ thống của các cơ quan, tổ chức, đặc biệt các cuộc tấn công vào cổng thông tin điện tử của cơ quan, tổ chức nhà nước để đưa nội dung hình ảnh độc hại không chỉ ảnh hưởng đến tổ chức mà còn gây ảnh hưởng đến không gian mạng Việt Nam. (Thông tin chi tiết về các hệ thống đã bị tấn công trong tháng được cập nhật tại phụ lục 4 kèm theo).

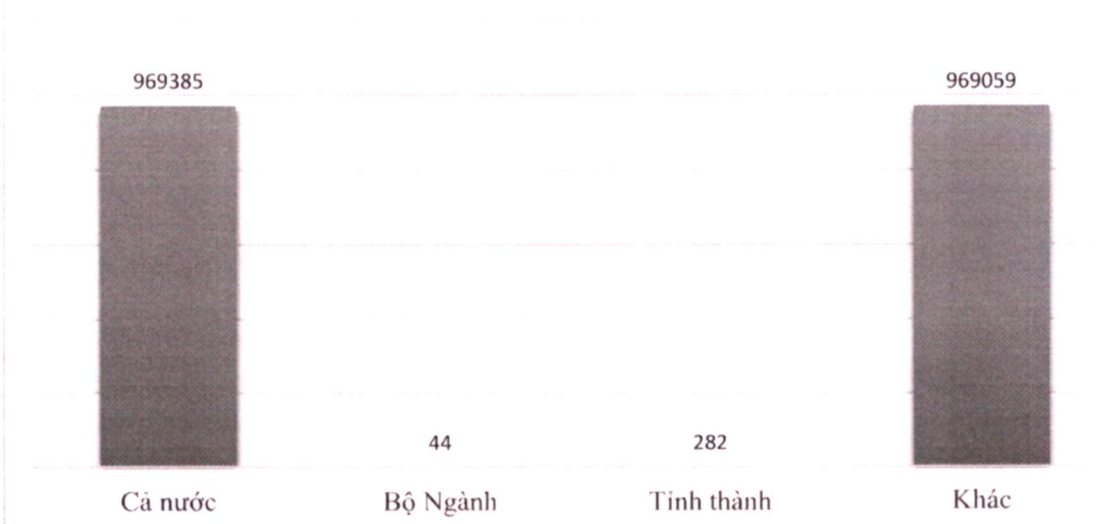
Bên cạnh đó, để tăng mức uy tín của website cơ quan nhà nước đối với người dân, đồng thời hỗ trợ ngăn chặn việc lợi dụng tên miền thực hiện kiểm tra, đánh giá mức độ an toàn thông tin của các website của cơ quan nhà nước (.gov.vn) thông qua việc chứng nhận tín nhiệm mạng. Trong thời gian qua, đã có nhiều cơ quan nhà nước thực hiện việc gắn nhãn lên website để đảm bảo được tín nhiệm mạng. Danh sách chi tiết các đơn vị được cập nhật tại phụ lục 5 kèm theo).

2. Tình hình lây nhiễm mã độc trên cả nước

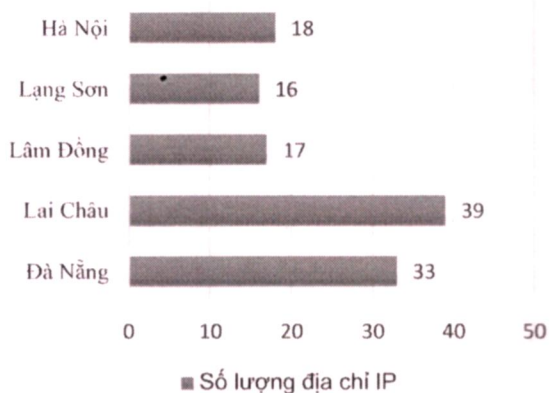
Trong tháng, Hệ thống kỹ thuật của Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC) đã ghi nhận 969.385 địa chỉ IP của Việt Nam nằm trong mạng botnet, trong đó có 326 địa chỉ IP của cơ quan, tổ chức nhà nước (44 địa chỉ IP Bộ/Ngành, 282 địa chỉ IP Tỉnh/Thành) giảm 2,37% so với tháng 11/2021.

Danh sách các đơn vị có địa chỉ IP nằm trong mạng botnet mà Trung tâm NCSC phát hiện có tại phụ lục 3 kèm theo.

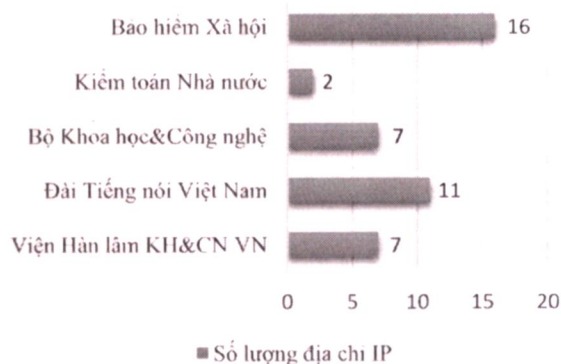
Số lượng địa chỉ IP nằm trong mạng botnet



Thống kê số lượng mã độc/botnet tại một số địa phương



Thống kê số lượng mã độc/botnet Bộ ngành và cơ quan trực thuộc Chính phủ



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 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.

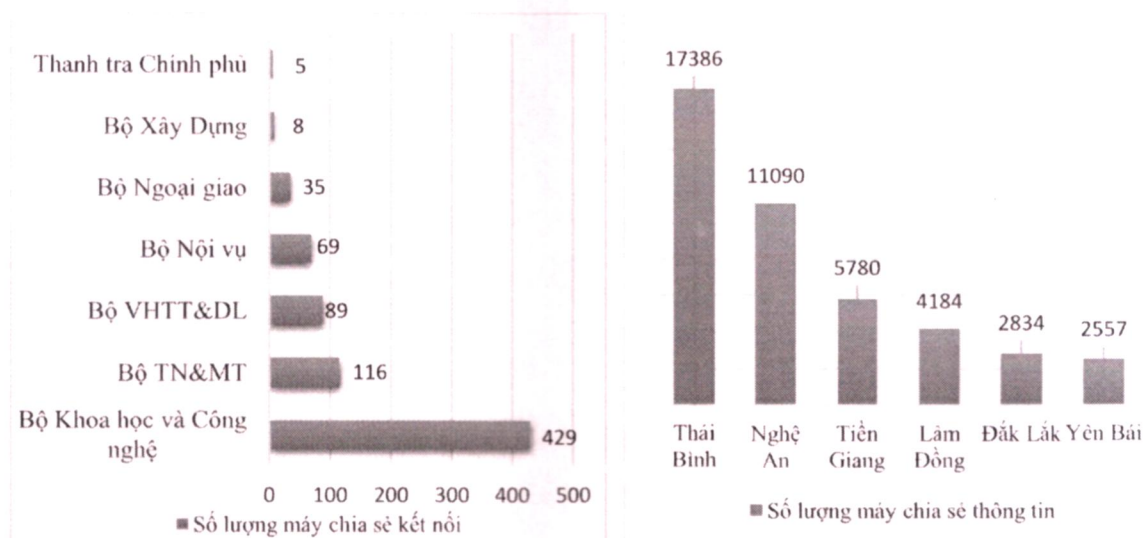
3. Tình hình chia sẻ dữ liệu theo Chỉ thị 14/CT-TTg 2018

Bên cạnh việc giám sát từ xa dựa trên dải địa chỉ IP tĩnh do Bộ/Ngành, Tỉnh/Thành cung cấp, Cục ATTT hiện đã triển khai kết nối chia sẻ thông tin về mã độc theo chỉ đạo tại 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.

Đến hết tháng 12/2021 đã có 83 đơn vị (62 Tỉnh/Thành, 21 Bộ/Ngành) thực hiện kết nối chia sẻ thông tin về mã độc với Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC).

Mặc dù có 83 đơn vị đã thực hiện kết nối chia sẻ thông tin về mã độc với Trung tâm NCSC, tuy nhiên hệ thống kỹ thuật của Trung tâm thống kê, ghi nhận chỉ có 61.965 máy có cài đặt giải pháp phòng chống mã độc và chia sẻ thông tin (liên quan đến hệ điều hành, mã độc, điểm yếu, kết nối nghi ngờ) trong tháng 12 vừa qua.

Một số đơn vị có số lượng máy chia sẻ kết nối trong tháng 11 tương đối đầy đủ:



4. Thông tin chung điểm yếu lỗ hổng

Trong tháng, Hệ thống kỹ thuật của Trung tâm đã ghi nhận có **1.357** điểm yếu, lỗ hổng an toàn thông tin tại các hệ thống thông tin của các cơ quan tổ chức nhà nước. Lỗ hổng gây mất an toàn thông tin tồn tại trên nhiều máy tính đã kết nối, chia sẻ thông tin.

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	Ghi chú
1	• CVE-2019-0708	Tham khảo Báo cáo tháng 9/2019
2	CVE-2020-0655	https://msrc.microsoft.com/update-guide/en-us/vulnerability/CVE-2020-0655
3	MS14-019	https://docs.microsoft.com/en-us/security-updates/securitybulletins/2014/ms14-019
4	CVE-2015-0009	Tham khảo Báo cáo tháng 9/2019

	(MS15-014)	
5	MS17-010	https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010

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

Nơi nhận:

- Hệ thống các đơn vị chuyên trách về ATTT/CNTT của các bộ, ngành, Sở TT&TT các tỉnh, thành phố trực thuộc Trung ương;
- Cục trưởng (đề b/c);
- Lưu: VT, NCSC.

**TL. CỤC TRƯỞNG
Q. GIÁM ĐỐC
TRUNG TÂM GIÁM SÁT AN TOÀN
KHÔNG GIAN MẠNG QUỐC GIA**



Trần Quang Hưng

Phụ lục I**DANH SÁCH CÁC ĐƠN VỊ CHƯA TRIỂN KHAI GIẢI PHÁP PHÒNG
CHỐNG MÃ ĐỘC ĐÁP ỨNG YÊU CẦU CỦA CHỈ THỊ SỐ 14/CT-TTg
NĂM 2018**

(Chưa kết nối chia sẻ dữ liệu về Cục ATTTT)

1. Đối với Bộ/Ngành

TT	Bộ/Cơ quan ngang Bộ/ Cơ quan trực thuộc Chính phủ
1	Bộ Công Thương
2	Bộ Giáo dục và Đào tạo
3	Bộ LĐTB&XH
4	Bộ Nông nghiệp và Phát triển nông thôn
5	Ủy ban Dân tộc
6	Viện Hàn lâm Khoa học Xã hội

2. Đối với Tỉnh/Thành

TT	Tỉnh/Thành
1	Bình Dương

Ghi chú: Thông tin về các Bộ/Ngành, Tỉnh/Thành chưa thực hiện kết nối chia sẻ thông tin về mã độc sẽ được Cục ATTT tổng hợp, báo cáo hàng tháng nhằm đơn đốc việc thực hiện chỉ tiêu mà Chính phủ đưa ra tại Nghị quyết 01/NQ-CP ngày 01/01/2020 của Chính phủ. Cụ thể: "90% các bộ, ngành, địa phương kết nối với Trung tâm Giám sát an toàn không gian mạng quốc gia".

Phụ lục II

**DANH SÁCH ĐIỂM YẾU LỖ HỒNG BẢO MẬT ĐÃ CÓ HỖ TRỢ
KỸ THUẬT**

STT	Mã điểm yếu/ lỗ hổng	Ghi chú
1	CVE-2019-0708	Tham khảo Báo cáo tháng 8/2019
2	CVE-2013-3900 (MS13-098)	Tham khảo Báo cáo tháng 8/2019
3	CVE-2014-4114 (MS14-060)	Tham khảo Báo cáo tháng 8/2019 Sandworm APT
4	CVE-2015-0009 (MS15-014)	Tham khảo Báo cáo tháng 9/2019
5	CVE-2015-1635 (MS15-034)	Tham khảo Báo cáo tháng 9/2019
6	CVE-2015-0084 (MS15-028)	Tham khảo Báo cáo tháng 9/2019
7	CVE-2014-0315 (MS14-019)	Tham khảo Báo cáo tháng 10/2019
8	CVE-2017-0144 (MS17-010)	Tham khảo Báo cáo tháng 10/2019
9	CVE-2013-3129 (MS13-053)	Tham khảo Báo cáo tháng 11/2019
10	CVE-2015-0073 (MS15-025)	Tham khảo Báo cáo tháng 11/2019
11	CVE-2015-0080 (MS15-024)	Tham khảo Báo cáo tháng 11/2019
12	CVE-2015-0076 (MS15-029)	Tham khảo Báo cáo tháng 12/2019
13	CVE-2013-3940 (MS13-089)	Tham khảo Báo cáo tháng 12/2019
14	CVE-2015-0012 (MS15-017)	Tham khảo Báo cáo tháng 12/2019
15	CVE-2014-0260 (MS14-001)	Tham khảo Báo cáo tháng 01/2020
16	CVE-2014-1818 (MS14-036)	Tham khảo Báo cáo tháng 01/2020
17	CVE-2014-6352 (MS14-064)	Tham khảo Báo cáo tháng 01/2020 Moonsoon APT
18	CVE -2014-0263 (MS14-007)	Tham khảo Báo cáo tháng 02/2020

19	CVE-2014-4148 (MS14-058)	Tham khảo Báo cáo tháng 02/2020 APT 31
20	CVE-2015-0078 (MS15-023)	Tham khảo Báo cáo tháng 02/2020
21	CVE-2008-4250 (MS08-067)	Tham khảo Báo cáo Tháng 03/2020 Silence APT
22	CVE-2014-2778 (MS14-034)	Tham khảo Báo cáo Tháng 03/2020
23	CVE-2013-3891 (MS13-086)	Tham khảo Báo cáo Tháng 03/2020

Phụ lục III
DANH SÁCH CÁC ĐƠN VỊ PHÁT HIỆN CÓ ĐỊA CHỈ IP NẪM TRONG
MẠNG BOTNET

1. Danh sách Tỉnh thành

TT	Tên đơn vị	Số lượng Ip botnet tháng 11	Số lượng Ip botnet tháng 12	Loại mã độc/botnet
1	Đà Nẵng	26	33	Conficker
2	Lai Châu	35	39	Lethic, Avalanche, Conficker
3	Thanh Hóa	12	11	Avalanche
4	Hà Nội	20	18	Lethic, Avalanche
5	Lâm Đồng	14	17	Avalanche
6	Long An	11	12	Lethic, Avalanche
7	Lạng Sơn	14	16	Lethic, Necurs, Avalanche
8	Điện Biên	0	9	Lethic, Avalanche
9	Nam Định	10	8	Avalanche
10	Hà Nam	6	8	Wannacry, Lethic, Avalanche
11	Nghệ An	5	3	Lethic, Wannacry, Other, Avalanche
12	Đồng Tháp	6	6	Avalanche

13	Gia Lai	9	7	Avalanche
14	Bình Thuận	3	5	Necurs, Stealrat, Avalanche
15	Ninh Bình	9	8	Avalanche, Wannacry
16	Lào Cai	5	6	Avalanche
17	Quảng Ninh	5	5	Avalanche, Lethic
18	Hung Yên	3	2	Other, Wannacry, Lethic, Avalanche
19	Hải Phòng	2	3	Wannacry, Stealrat, Other, Avalanche
20	Thái Bình	3	4	Avalanche
21	Đắk Nông	7	7	Avalanche, Other
22	Bà Rịa Vũng Tàu	2	3	Avalanche
23	Tiền Giang	3	4	Wannacry, Lethic, Avalanche
24	Tuyên Quang	4	3	Avalanche, Conficker
25	Đắk Lắk	3	3	
26	Cao Bằng	2	2	Avalanche
27	Cần Thơ	2	4	Wannacry, Lethic, Avalanche
28	Hà Tĩnh	3	4	Wannacry, Lethic, Avalanche

29	Bình Dương	2	2	Lethic, Emotet, Necurs, Avalanche
30	Quảng Trị	1	1	Avalanche
31	Bình Phước	3	2	Avalanche, Conficker
32	Bến Tre	1	2	Avalanche
33	Hòa Bình	2	1	Avalanche
34	Kon Tum	3	3	Avalanche, Wannacry
35	Bắc Kạn	2	0	Avalanche, Wannacry
36	Phú Thọ	1	1	
37	Yên Bái	2	3	Lethic, Avalanche
38	Vĩnh Phúc	4	3	Avalanche
39	Vĩnh Long	3	0	Avalanche
40	Đồng Nai	1	1	Avalanche
41	An Giang	4	5	Avalanche
42	Hà Giang	7	9	Lethic, Avalanche

2. Danh sách Bộ ngành

TT	Tên đơn vị	Số lượng IP botnet tháng 11	Số lượng IP botnet tháng 12	Loại mã độc/botnet
1	Đài Tiếng nói Việt Nam	11	11	
2	Viện Hàn lâm khoa học và Công nghệ Việt Nam	06	07	Avalanche, Ponyloaders
3	Bộ Khoa học và Công nghệ	05	07	Avalanche
4	Kiểm toán Nhà nước	02	02	Avalanche
5	Bảo hiểm Xã hội	08	16	
6	Bộ Tư Pháp	01	01	Avalanche

Phụ lục IV
DANH SÁCH WEBSITE (.gov.vn) BỊ TẤN CÔNG TRONG THÁNG

TT	Website/Đường dẫn	Đơn bị chuyên trách	Đơn vị quản lý/sử dụng	24 giờ chưa xử lý	48 giờ chưa xử lý	Đã xử lý
1	http://tuphap.hatinh.gov.vn/Morocco.txt		Sở Tư Pháp Hà Tĩnh			x
2	http://ncerwass.mard.gov.vn/pride.txt	Bộ Nông nghiệp & Phát triển Nông thôn	Trung tâm Quốc gia nước sạch và vệ sinh môi trường nông thôn - Tổng cục Thủy lợi			x
3	http://bantindientu.mard.gov.vn/pride.txt	Bộ Nông nghiệp & Phát triển Nông thôn	Cổng thông tin điện tử			x

Ghi chú: Một số nguồn thông tin công khai cán bộ chuyên trách tại các đơn vị có thể chủ động theo dõi để có phương án xử lý sớm nhất gồm:

- <http://www.zone-h.org>
- <http://phishtank.org>

Phụ lục V
DANH SÁCH CÁC ĐƠN VỊ CHUYÊN TRÁCH VỀ CNTT/ATTT ĐÃ
ĐĂNG KÝ TÍN NHIỆM WEBSITE CHO CƠ QUAN NHÀ NƯỚC

1. Danh sách Bộ Ngành

TT	Tên đơn vị	Số lượng website đã đăng kí	Số lượng website đạt yêu cầu cấp nhãn tín nhiệm	Số lượng website đã gán nhãn
1	Bộ Giao thông Vận tải	38	23	05
2	Bộ Khoa học và Công nghệ	06	06	06
3	Bộ Lao động&Thương binh Xã hội	1	0	0
4	Bộ Ngoại giao	95	95	0
5	Bộ Nội vụ	11	11	0
6	Bộ Nông nghiệp Phát triển Nông thôn	53	6	3
7	Bộ Tư Pháp	104	57	57
8	Bộ Y tế	15	11	06
9	Ngân hàng Nhà Nước	11	06	06
10	Ban Quản lý Lăng	02	02	02
11	Bảo hiểm Xã hội	75	75	73
12	Đài Truyền hình VN	01	01	01
13	Viện Hàn lâm KHCN	03	01	0
14	Viện Hàn lâm KHXH VN	39	32	0

15	Văn phòng Quốc hội	06	03	0
----	--------------------	----	----	---

2. Danh sách Tỉnh thành

TT	Tên đơn vị	Số lượng website đã đăng kí	Số lượng website đạt yêu cầu cấp nhân tín nhiệm	Số lượng website đã gán nhãn
1	Bắc Giang	49	37	0
2	Bắc Kạn	25	23	13
3	Bắc Ninh	163	49	0
4	Bà Rịa – Vũng Tàu	86	48	38
5	Bến Tre	46	35	17
6	Bình Định	33	03	0
7	Bình Dương	29	15	0
8	Bình Phước	43	20	0
9	Bình Thuận	38	34	34
10	Cao Bằng	43	02	01
11	Đắk Lắk	38	04	01
12	Đắk Nông	11	11	02
13	Gia Lai	28	28	01
14	Hải Dương	273	12	10
15	Hà Nội	38	93	29
16	Hà Nam	220	27	0
17	Hậu Giang	03	03	03

18	Hưng Yên	54	30	0
19	Khánh Hòa	146	103	02
20	Kiên Giang	633	50	0
21	Lai Châu	05	03	03
22	Lạng Sơn	03	03	03
23	Lào Cai	54	54	20
24	Long An	48	47	47
25	Nam Định	238	238	107
26	Nghệ An	54	01	0
27	Ninh Bình	122	24	20
28	Ninh Thuận	15	02	01
29	Quảng Ngãi	34	34	34
30	Sóc Trăng	66	65	65
31	Sơn La	45	38	34
32	Thái Bình	286	26	0
33	Thái Nguyên	25	01	01
34	Thanh Hóa	25	25	24
35	Thừa Thiên Huế	315	278	185
36	Trà Vinh	193	49	0
37	Vĩnh Long	119	119	119
38	Vĩnh Phúc	38	16	0
39	Yên Bái	44	37	34

40	An Giang	42	40	40
41	Quảng Bình	33	33	01
42	Lâm Đồng	01	01	01
43	Phú Thọ	01	01	0
44	Tiền Giang	01	01	01
45	Cần Thơ	108	28	15
46	Đà Nẵng	163	56	0
47	Đồng Tháp	83	66	0
48	Quảng Ninh	68	47	17
49	Tây Ninh	53	44	36
50	Điện Biên	34	03	02

Ghi chú: Số lượng website đã đăng kí được thống kê căn cứ vào công văn gửi về từ các đơn vị.