UBND TỈNH QUẢNG NGÃI
SỞ GIÁO DỤC VÀ ĐÀO TẠO

Số: 272 /TB-SGDĐT

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập – Tự do – Hạnh phúc

Quảng Ngãi, ngày 22 tháng 02 năm 2022

THÔNG BÁO
Tình hình an toàn thông tin tháng 01/2022 và thống kê kết nối chia sẻ thông tin về mã độc

Theo thông tin của Cục An toàn thông tin tại Báo cáo số 02/BC-CATTT ngày 16/02/2022 về Báo cáo Kỹ thuật Tình hình an toàn thông tin tháng 01/2022 và thống kê kết nối chia sẻ thông tin về mã độc, Sở Thông tin và Truyền thông tại Công văn số 189/STTTT-BCVT&CNTT ngày 21/02/2022, Sở Giáo dục và Đào tạo thông báo đến các đơn vị, cơ sở giáo dục nắm tình hình, triển khai thông tin đến các cán bộ, giáo viên thực hiện các biện pháp để hạn chế các rủi ro về nguy cơ mất an toàn thông tin.

(Kèm theo báo cáo kỹ thuật của Cục An toàn thông tin)

Yêu cầu lãnh đạo các đơn vị quan tâm chỉ đạo thực hiện./.

***Nơi nhận*:**
- Đơn vị trực thuộc Sở GDĐT;
- Phòng GDĐT huyện, thị xã, thành phố;
- Trung tâm GDNN-GDTX huyện, thị xã;
- Lãnh đạo Sở GDĐT;
- Các phòng thuộc Sở GDĐT;
- Lưu: VT, VP, ndh.

TL. GIÁM ĐỐC
KT. CHÁNH VĂN PHÒNG
PHÓ CHÁNH VĂN PHÒNG

CỘNG HÒA X.H.C.N VIỆT NAM
SỞ GIÁO DỤC VÀ ĐÀO TẠO
TỈNH QUẢNG NGÃI

Nguyễn Đức Huân

BỘ THÔNG TIN VÀ TRUYỀN THÔNG
CỤC AN TOÀN THÔNG TIN

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

Số: **02**/BC-CATTT

Hà Nội, ngày 16 tháng 02 năm 2022

BÁO CÁO KỸ THUẬT
Tình hình an toàn thông tin tháng 01/2022 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

Cảnh báo số 56/CATTT-NCSC ngày 12/01/2022 về việc các lỗ hổng bảo mật ảnh hưởng mức cao và nghiêm trọng trong các sản phẩm Microsoft tháng 01/2022.

Cảnh báo số 144/CATTT-NCSC ngày 27/01/2022 về việc lỗ hổng bảo mật CVE-2021-4034 trong Polkit pkexec ảnh hưởng nghiêm trọng đến hệ điều hành Linux.

Nhằm hỗ trợ kịp thời các cơ quan, tổ chức trong công tác đảm bảo an toàn thông tin, bên cạnh hoạt động dự báo, 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 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 gây ảnh hưởng xấu đến tổ chức và 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).

Ghi chú: Lưu hành nội bộ.

Bên cạnh đó, để tăng mức uy tín của website cơ quan nhà nước đối với người dân, Trung tâm Giám sát an toàn không gian mạng quốc gia còn 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. Danh sách chi tiết việc cấp nhãn tín nhiệm cho website của cơ quan nhà nước được cập nhật tại Phụ lục 6 kèm theo).

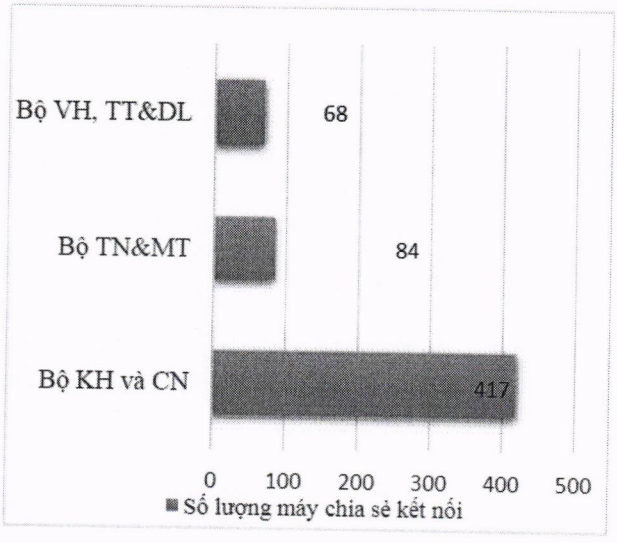
2. Tình hình triển khai công tác phòng chống phần mềm độc hại và chia sẻ dữ liệu mã độc theo Chỉ thị 14/CT-TTg năm 2018

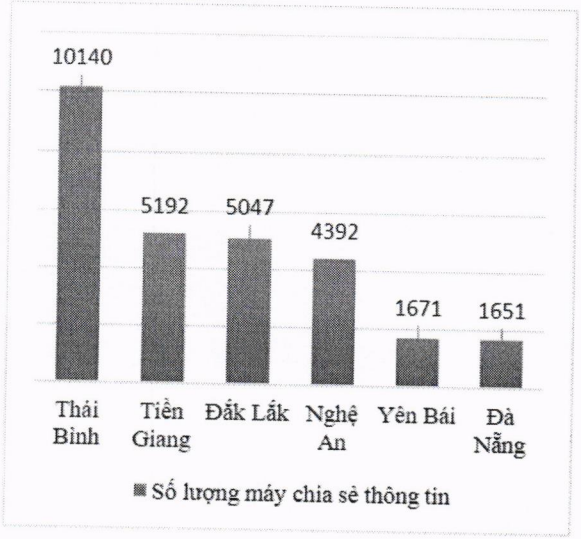
Thực hiện Chỉ thị số 14/CT-TTg của Thủ tướng Chính phủ ban hành ngày 25/5/2018 về việc nâng cao năng lực phòng, chống phần mềm độc hại, Cục An toàn thông tin đã giao Trung tâm Giám sát an toàn không gian mạng quốc gia hỗ trợ **13** doanh nghiệp có giải pháp phòng chống mã độc thực hiện kết nối chia sẻ 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.

Đến hết tháng **01/2022** đã có **83** đơn vị (62 Tỉnh/Thành, 21 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 **01/2022,** thông qua kết nối chia sẻ dữ liệu về mã độc từ **83** đơn vị, Hệ thống kỹ thuật của Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC) ghi nhận có **25.330** 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).

Một số đơn vị có số lượng máy chia sẻ kết nối trong tháng 01 tương đối đầy đủ:





Ghi chú: Lưu hành nội bộ.

Ghi chú: 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 tai Phụ lục 1 kèm theo.

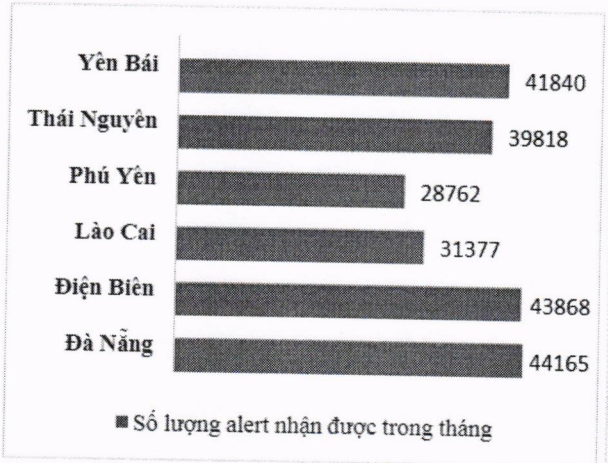
3. Tình hình triển khai công tác giám sát an toàn thông tin và kết nối chia sẻ dữ liệu giám sát theo Chỉ thị 14/CT-TTg năm 2019

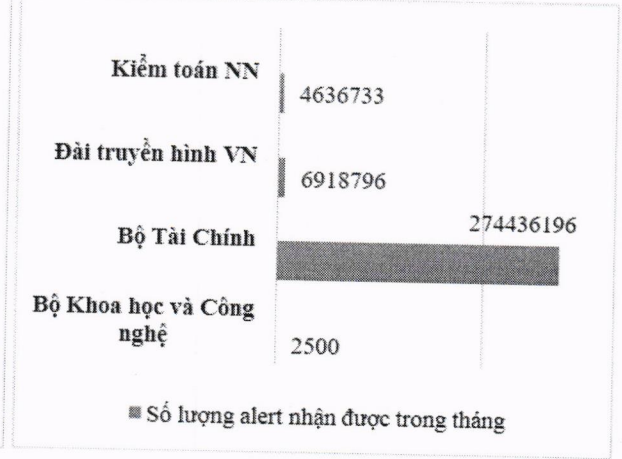
Thực hiện Chỉ thị số 14/CT-TTg của Thủ tướng Chính phủ ban hành ngày 07/6/2019 về việc tăng cường bảo đảm an toàn, an ninh mạng nhằm cải thiện chỉ số xếp hạng của Việt Nam, Cục An toàn thông tin đã giao Trung tâm Giám sát an toàn không gian mạng quốc gia hỗ trợ **13** doanh nghiệp có giải pháp giám sát 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.

Đến hết tháng **01/2022** 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 **01/2022,** 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 **39/87** đơn vị có kết nối chia sẻ dữ liệu tương đối đầy đủ, **48/87** 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:





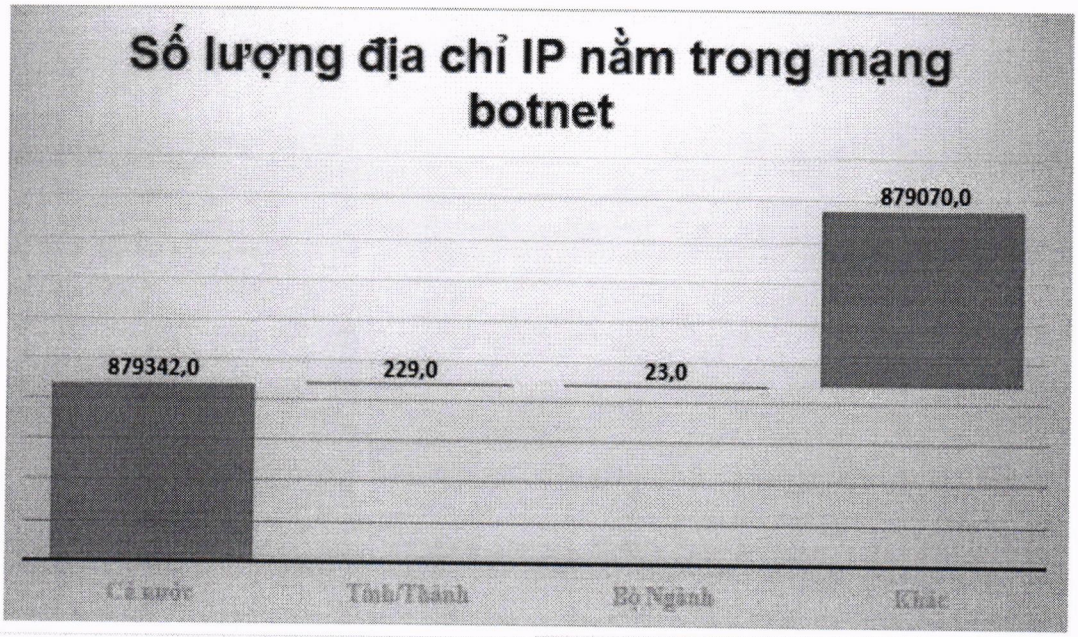
Ghi chú: Hiện trạng kết nối chia sẻ dữ liệu giám sát tại Phụ lục 2 kèm theo.

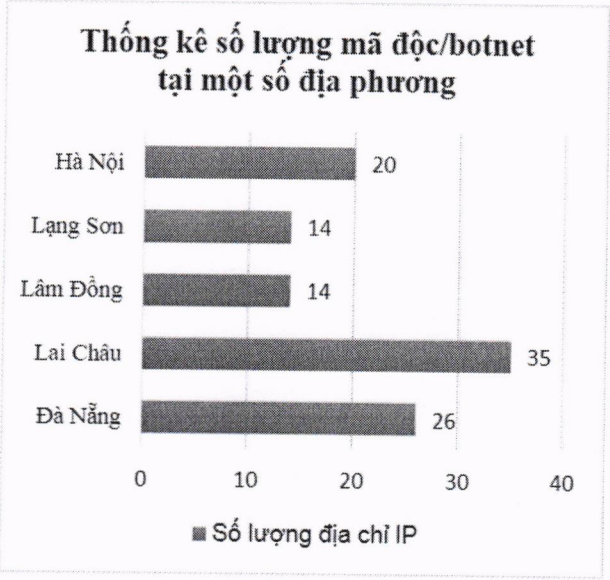
4. Tình hình lây nhiễm mã độc trên cả nước

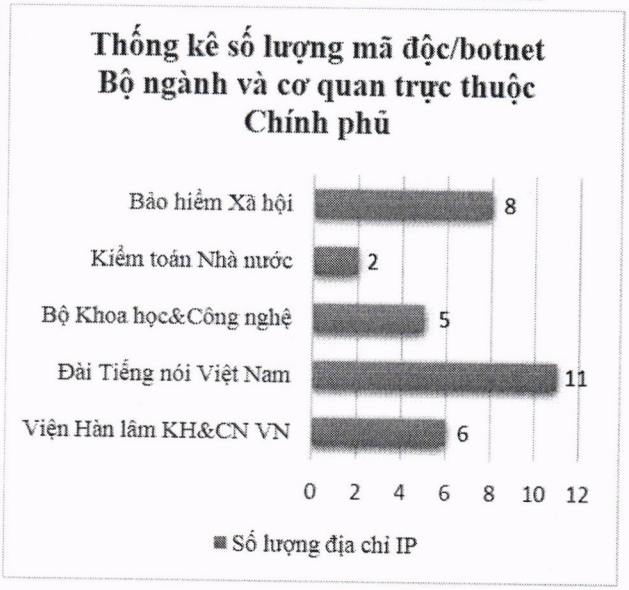
Trong tháng, Hệ thống kỹ thuật của Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC) đã ghi nhận 879.342 địa chỉ IP của Việt Nam nằm

trong mạng botnet, trong đó có 252 địa chỉ IP của cơ quan, tổ chức nhà nước (23 địa chỉ IP Bộ/Ngành, 229 địa chỉ IP Tỉnh/Thành) giảm 9.29 % so với tháng 12/2021.

Ghi chú: Lưu hành nội bộ.







Ghi chú: *Danh sách các đơn vị có địa chỉ IP nằm trong mạng botnet Trung tâm NCSC phát hiện có tại phụ lục 3 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. 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 **1.257** 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	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 (MS15-014)	Tham khảo Báo cáo tháng 9/2019
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, tổ chức 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 (để 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

Ghi chú: Lưu hành nội bộ.

Phụ lục II

TÌNH HÌNH KẾT NỐI, CHIA SẺ DỮ LIỆU GIÁM SÁT VỀ CỤC AN TOÀN THÔNG TIN THEO YÊU CẦU CHỈ THỊ SỐ 14/CT-TTG NĂM 2019

1. Danh sách Bộ/Ngành

TT	Bộ/Ngành/Cơ quan trực thuộc Chính phủ	Thời gian bắt đầu chia sẻ dữ liệu	Thời gian gần nhất nhận được dữ liệu (tính đến 31/01/2022)
1	Bộ Công Thương	09/08/2020	14/02/2021
2	Bộ Giáo dục và Đào tạo	31/08/2020	14/10/2021
3	Bộ Giao thông vận tải	15/05/2020	29/06/2020
4	Bộ Kế hoạch và Đầu tư	20/11/2020	19/09/2021
5	Bộ Khoa học và Công nghệ	19/11/2020	06/02/2021
6	Bộ Lao động - Thương Binh và Xã hội	11/12/2020	01/01/2022
7	Bộ Ngoại giao	24/07/2020	18/09/2020
8	Bộ Nội vụ	30/07/2020	21/01/2021
9	Bộ Nông nghiệp và Phát triển nông thôn	28/09/2020	09/11/2021
10	Bộ Tài chính	15/12/2020	31/01/2022
11	Bộ Tài nguyên và Môi trường	03/10/2020	01/12/2021
12	Bộ Tư pháp	24/04/2020	15/10/2021
13	Bộ Văn hóa, Thể thao và Du lịch	20/06/2020	12/08/2020
14	Bộ Xây Dựng	23/07/2020	23/07/2020
15	Bộ Y tế	17/07/2020	14/08/2020
16	Ngân hàng Nhà nước Việt Nam	02/07/2020	28/09/2020
17	Thanh tra Chính phủ	10/11/2020	06/07/2021
18	Ủy ban Dân tộc	08/10/2020	08/10/2020
19	Văn phòng Chính phủ	22/09/2020	27/01/2022

Ghi chú: Lưu hành nội bộ.

20	Bảo Hiểm Xã Hội	8/11/2020	21/07/2021
21	Đài Truyền hình Việt Nam	14/09/2020	31/01/2022
22	Viện Hàn Lâm KHCN	22/09/2020	28/03/2021
23	Kiểm toán Nhà nước Việt Nam	09/03/2021	15/01/2022

2. Danh sách Tỉnh/Thành

TT	Tỉnh/Thành	Thời gian bắt đầu chia sẻ dữ liệu	Thời gian gần nhất nhận được dữ liệu (tính đến 31/01/2022)
1	An Giang	30/09/2020	11/01/2021
2	Bắc Giang	21/08/2020	19/06/2021
3	Bắc Kạn	01/09/2020	20/01/2022
4	Bạc Liêu	09/10/2020	30/01/2022
5	Bắc Ninh	23/07/2020	16/06/2021
6	Bà Rịa - Vũng Tàu	20/07/2020	31/01/2022
7	Bến Tre	10/08/2020	30/01/2022
8	Bình Định	05/06/2020	08/04/2021
9	Bình Dương	24/04/2020	02/07/2020
10	Bình Phước	23/04/2020	27/01/2022
11	Bình Thuận	31/08/2020	31/01/2022
12	Cà Mau	15/05/2020	04/09/2020
13	Cần Thơ	13/04/2020	24/12/2021
14	Cao Bằng	14/08/2020	31/01/2022
15	Đắk Lắk	17/06/2020	31/01/2022
16	Đắk Nông	31/08/2020	31/01/2022
17	Đà Nẵng	09/06/2020	31/01/2022
18	Điện Biên	02/06/2020	31/01/2022
19	Đồng Nai	15/06/2020	30/06/2021
20	Đồng Tháp	14/07/2020	01/09/2020
21	Gia Lai	14/09/2020	27/09/2021

Ghi chú: Lưu hành nội bộ.

22	Hà Giang	18/08/2020	31/01/2022
23	Hải Dương	04/09/2020	09/03/2021
24	Hải Phòng	28/07/2020	31/01/2022
25	Hà Nam	22/09/2020	31/01/2022
26	Hà Nội	30/06/2020	20/10/2020
27	Hà Tĩnh	06/10/2020	31/01/2022
28	Hòa Bình	13/05/2020	29/06/2020
29	Hồ Chí Minh	26/06/2020	31/01/2022
30	Hậu Giang	02/10/2020	02/10/2020
31	Hưng Yên	22/05/2020	31/01/2022
32	Khánh Hòa	21/09/2020	31/01/2022
33	Kiên Giang	24/09/2020	31/01/2022
34	Kon Tum	28/09/2020	31/01/2022
35	Lai Châu	26/09/2020	06/10/2020
36	Lâm Đồng	22/10/2020	22/10/2020
37	Lạng Sơn	08/10/2020	01/01/2021
38	Lào Cai	09/07/2020	31/01/2022
39	Long An	22/07/2020	13/01/2022
40	Nam Định	21/09/2020	21/09/2021
41	Nghệ An	09/09/2020	31/01/2022
42	Ninh Bình	28/07/2020	10/08/2020
43	Ninh Thuận	01/09/2020	31/01/2022
44	Phú Thọ	01/10/2020	05/10/2020
45	Phú Yên	30/11/2020	31/01/2022
46	Quảng Bình	01/07/2020	02/12/2021
47	Quảng Nam	14/09/2020	31/01/2022
48	Quảng Ngãi	12/08/2020	31/01/2022
49	Quảng Ninh	12/09/2020	05/11/2020
50	Quảng Trị	24/12/2020	24/12/2020
51	Sóc Trăng	12/08/2020	19/10/2020

Ghi chú: Lưu hành nội bộ.

52	Sơn La	13/07/2020	28/06/2021
53	Tây Ninh	08/07/2020	10/11/2021
54	Thái Bình	25/06/2020	08/01/2021
55	Thái Nguyên	19/11/2020	31/01/2022
56	Thanh Hóa	29/09/2020	06/12/2021
57	Thừa Thiên Huế	29/07/2020	06/07/2021
58	Tiền Giang	24/09/2020	31/01/2022
59	Trà Vinh	29/07/2020	31/01/2022
60	Tuyên Quang	19/11/2020	06/10/2021
61	Vĩnh Long	25/06/2020	17/08/2021
62	Vĩnh Phúc	30/06/2020	31/07/2021
63	Yên Bái	26/08/2020	31/01/2022

Ghi chú: Lưu hành nội bộ.

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

1. Danh sách Bộ/Ngành

TT	Tên đơn vị	Số lượng IP botnet tháng 12/2021	Số lượng IP botnet tháng 01/2022	Loại mã độc/botnet
1	Đài Tiếng nói Việt Nam	11	10	
2	Viện Hàn lâm khoa học và Công nghệ Việt Nam	7	0	
3	Bộ Khoa học và Công nghệ	7	6	Avalanche
4	Kiểm toán Nhà nước	2	2	Avalanche
5	Bảo hiểm Xã hội	16	3	
6	Bộ Tư Pháp	1	1	Avalanche
7	Bộ Y tế	0	1	

2. Danh sách Tỉnh/thành

TT	Tên đơn vị	Số lượng Ip botnet tháng 12/2021	Số lượng Ip botnet tháng 01/2022	Loại mã độc/botnet
1	Đà Nẵng	33	57	Conficker
2	Lai Châu	39	19	Lethic, Avalanche, Conficker

Ghi chú: Lưu hành nội bộ.

3	Thanh Hóa	11	9	Avalanche
4	Hà Nội	18	14	Lethic, Avalanche
5	Lâm Đồng	17	10	Avalanche
6	Long An	12	4	Lethic, Avalanche
7	Lạng Sơn	16	10	Lethic, Necurs, Avalanche
8	Điện Biên	9	6	Lethic, Avalanche
9	Nam Định	8	8	Avalanche
10	Hà Nam	8	10	Wannacry, Lethic, Avalanche
11	Nghệ An	3	2	Lethic, Wannacry, Other, Avalanche
12	Đồng Tháp	6	6	Avalanche
13	Gia Lai	7	3	Avalanche
14	Bình Thuận	5	1	Necurs, Stealrat, Avalanche
15	Ninh Bình	8	7	Avalanche, Wannacry
16	Lào Cai	6	5	Avalanche
17	Quảng Ninh	5	3	Avalanche, Lethic
18	Hưng Yên	2	2	Other, Wannacry,

Ghi chú: Lưu hành nội bộ.

				Lethic, Avalanche
19	Hải Phòng	3	2	Wannacry, Stealrat, Other, Avalanche
20	Thái Bình	4	3	Avalanche
21	Đắk Nông	7	6	Avalanche, Other
22	Bà Rịa Vũng Tàu	3	0	
23	Tiền Giang	4	3	Wannacry, Lethic, Avalanche
24	Tuyên Quang	3	2	Avalanche, Conficker
25	Đắk Lắk	3	4	
26	Cao Bằng	2	0	
27	Cần Thơ	4	6	Wannacry, Lethic, Avalanche
28	Hà Tĩnh	4	2	Wannacry, Lethic, Avalanche
29	Bình Dương	2	2	Lethic, Emotet, Necurs, Avalanche
30	Quảng Trị	1	2	Avalanche
31	Bình Phước	2	2	Avalanche, Conficker
32	Bến Tre	2	1	Avalanche
33	Hòa Bình	1	2	Avalanche

Ghi chú: Lưu hành nội bộ.

34	Kon Tum	3	2	Avalanche, Wannacry
35	Phú Thọ	1	1	
36	Yên Bái	3	3	Lethic, Avalanche
37	Vĩnh Phúc	3	3	Avalanche
38	Đồng Nai	1	0	
39	An Giang	5	4	Avalanche
40	Hà Giang	9	4	Lethic, Avalanche
41	Quảng Ngãi	0	1	
42	Sơn la	0	1	

Ghi chú: Lưu hành nội bộ.

Phụ lục IV
DANH SÁCH WEBSITE CƠ QUAN NHÀ NƯỚC (.GOV.VN) BỊ TẤN CÔNG TRONG THÁNG

TT	Website/Đường dẫn	Đơn vị chuyên trách	Đơn vị quản lý/sử dụng	24 giờ chưa xử lý	48 giờ chưa xử lý	Đã xử lý
1	http://sodulich.tphcm.gov.vn/web/kenhtonghopaz1	Sở TTTT Hồ Chí Minh				x
2	https://daklak.gov.vn/	Sở TTTT Đắk Lắk				x
3	https://cuakhauso.langson.gov.vn/ImageTestResult/	Sở TTTT Lạng Sơn				x
4	https://hpe.gov.vn/ http://hoaphuong.gov.vn/fck.html	Sở TTTT Hải Phòng				x
5	https://ited.gov.vn/su.txt		Viện Phát triển Công nghệ và Quản lý Giáo Dục	x	x	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