

Số: /BC-CATT

Hà Nội, ngày tháng năm 2022

## BÁO CÁO KỸ THUẬT

**Tình hình an toàn thông tin tháng 7/2022  
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

Văn bản số 1071/CATTT-NCSC về việc lỗ hổng bảo mật ảnh hưởng Cao trong các sản phẩm Microsoft công bố tháng 7/2022.



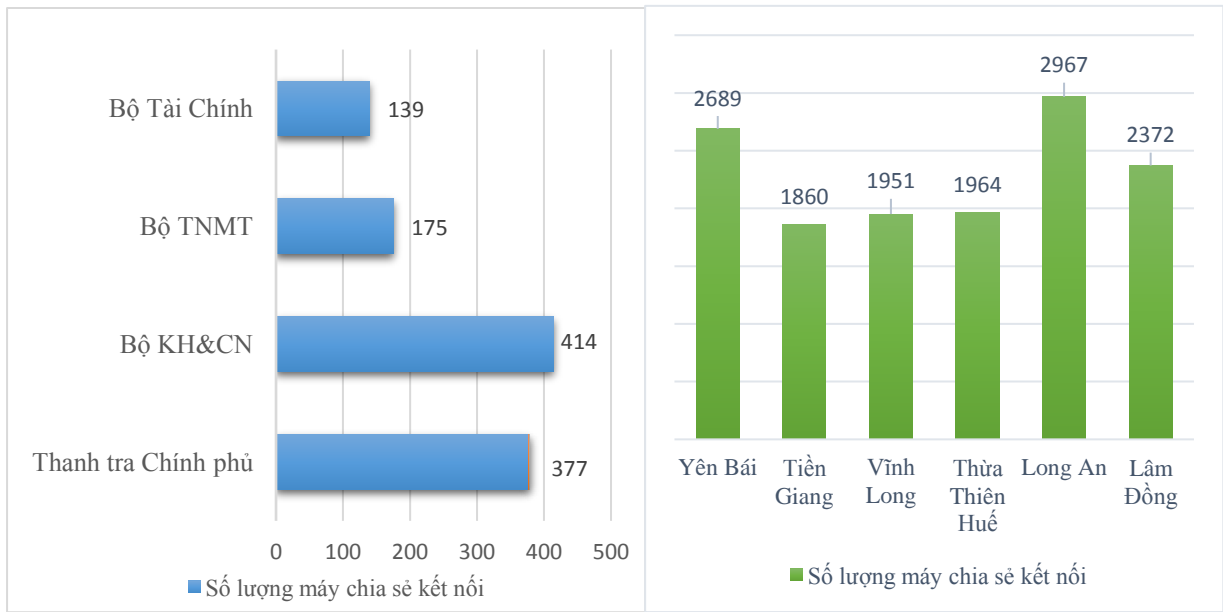
### 2. Tình hình triển khai công tác phòng chống phần mềm độc hại và chia sẻ dữ liệu mã độc theo Chỉ thị 14/CT-TTg năm 2018

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. Danh sách sản phẩm phòng chống mã độc có khả năng kết nối chia sẻ dữ liệu cập nhật tại: <https://www.ais.gov.vn/thong-tin-tham-khao/danh-sach-san-pham-phong-chong-ma-doc-co-kha-nang-ket-noi-chia-se-du-lieu.htm>

Đến hết tháng 7/2022 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 7/2022, 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 73/83 đơn vị có kết nối thường xuyên, 62/73 đơn vị có chia sẻ về hệ điều hành các máy (tổng số máy là 57.662).

**Một số đơn vị có số lượng máy chia sẻ kết nối trong tháng 7 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 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

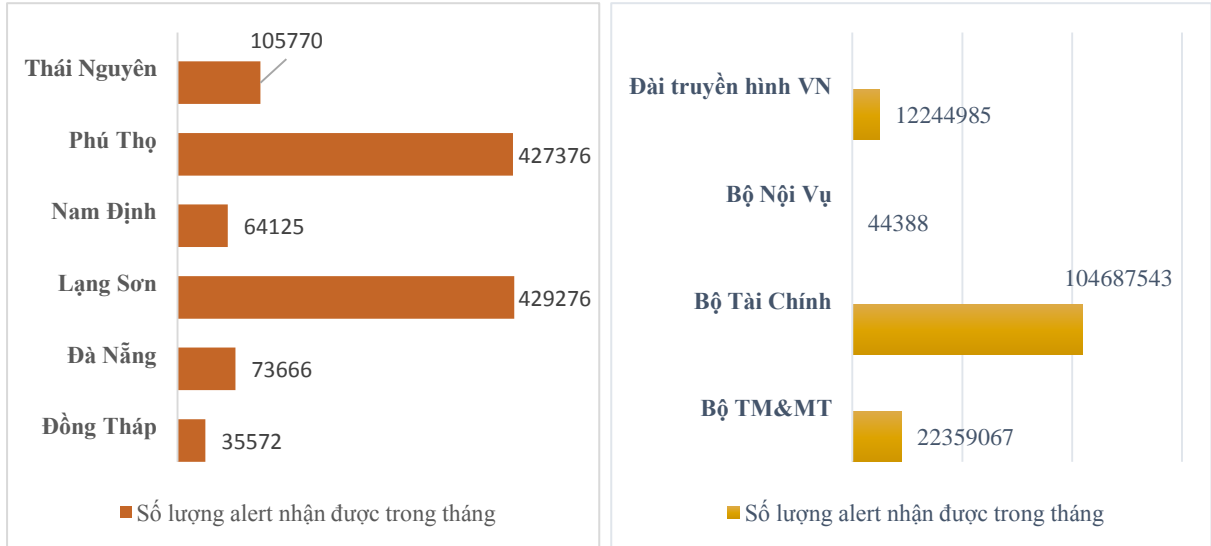
Thực hiện Chỉ thị số 14/CT-TTg của Thủ tướng Chính phủ ban hành ngày 07/6/2019 về việc tăng cường bảo đảm an toàn, an ninh mạng nhằm cải thiện chỉ số xếp hạng của Việt Nam, Cục An toàn thông tin đã giao Trung tâm Giám sát an toàn không gian mạng quốc gia hỗ trợ 13 doanh nghiệp có giải pháp giám sát an toàn thông tin thực hiện kết nối chia sẻ dữ liệu theo văn bản 2973/BTTTT-CATT 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 7/2022 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 7/2022, 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 **71/87** đơn vị có kết nối chia sẻ dữ liệu tương đối đầy đủ, **16/87** đơn vị bị mất kết nối chia sẻ dữ liệu.

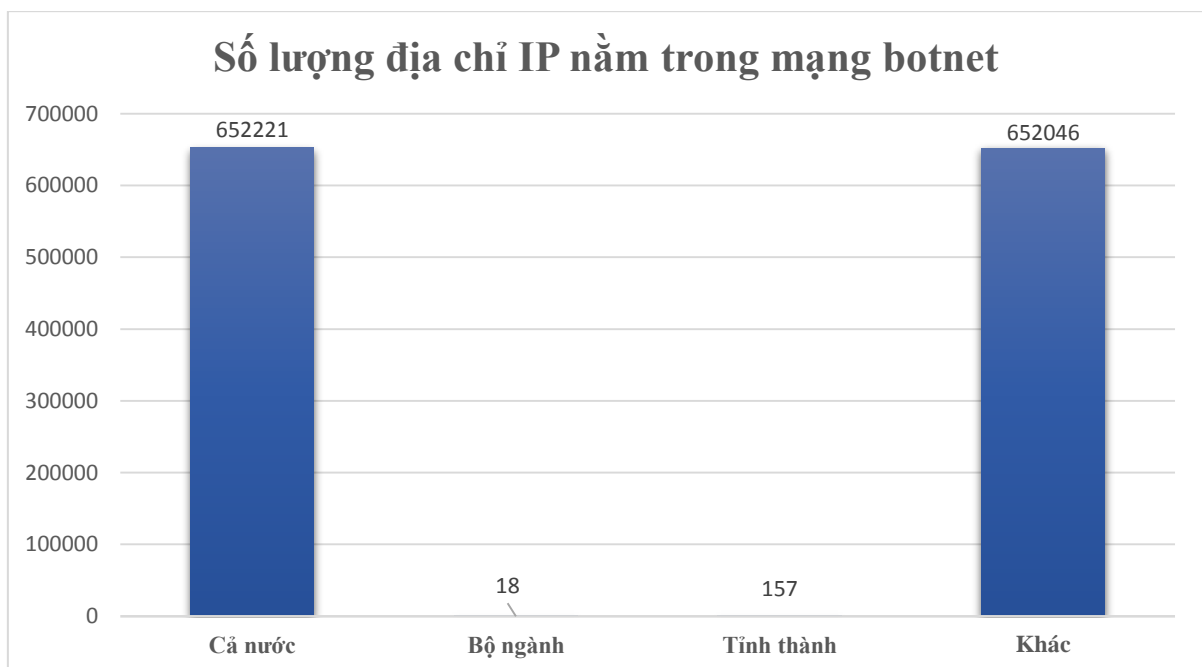
**Một số đơn vị có kết nối chia sẻ dữ liệu giám sát trong tháng tương đối đầy đủ:**

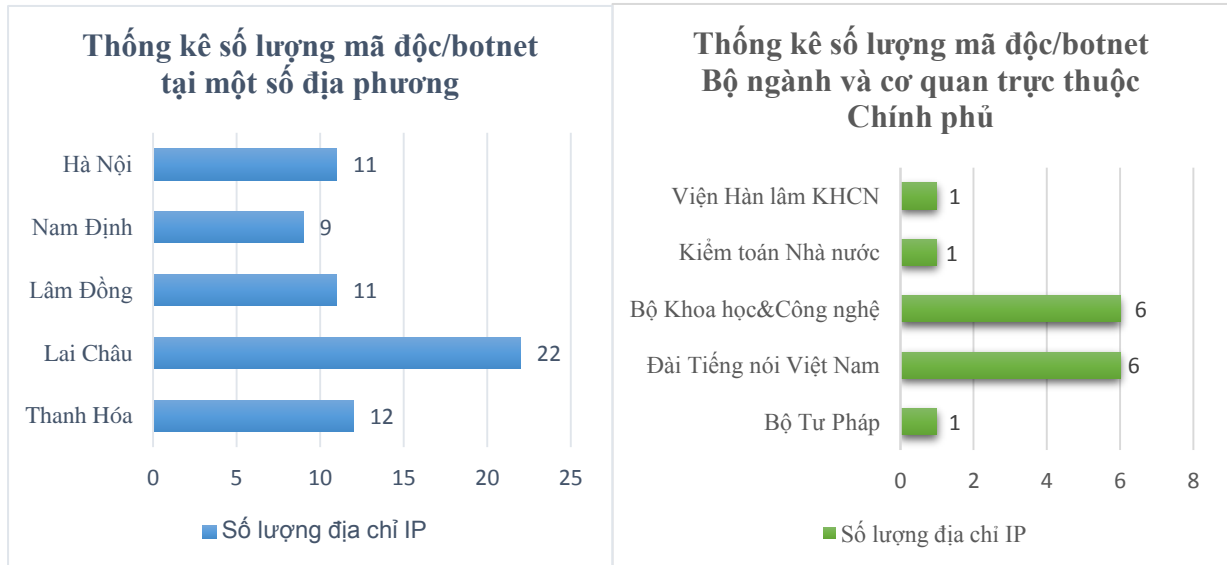


**Ghi chú:** Hiện trạng kết nối chia sẻ dữ liệu giám sát tại Phụ lục 2 kèm theo.

#### 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 652.221 địa chỉ IP của Việt Nam nằm trong mạng botnet (giảm 7.48% so với tháng 6/2022), trong đó có 175 địa chỉ IP của cơ quan, tổ chức nhà nước (18 địa chỉ IP Bộ/Ngành, 157 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 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 **1.851** 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-2018-11617	989	<a href="https://www.zerodayinitiative.com/advisories/ZDI-18-694/">https://www.zerodayinitiative.com/advisories/ZDI-18-694/</a>

2	CVE-2018-20250	817	<a href="https://nvd.nist.gov/vuln/detail/cve-2018-20250">https://nvd.nist.gov/vuln/detail/cve-2018-20250</a>
3	CVE-2022-21845	502	<a href="https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-21845">https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-21845</a>
4	CVE-2019-5126	460	<a href="https://talosintelligence.com/vulnerability_reports/TALOS-2019-0915">https://talosintelligence.com/vulnerability_reports/TALOS-2019-0915</a>
5	CVE-2020-9592	393	<a href="https://helpx.adobe.com/security/products/acrobat/apsb20-24.html">https://helpx.adobe.com/security/products/acrobat/apsb20-24.html</a>

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 16 kết nối nghi ngờ phát sinh trong tháng:

STT	IP/Domain độc hại	STT	IP/Domain độc hại
1	tawuhoju.com	7	1d0wnload1ngx.com
2	lookujie.net	8	freeprosoftz.com
3	mc7clurd09pla4nrtat7ion.com	9	d24ak3f2b.top
4	d24ak3f2b.top	10	tag.min.js
5	atomictrivia.ru	11	grootcho.com
6	disorderstatus.ru	12	ugroocuw.net

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 (đề b/c);
- Trung tâm VNCERT/CC, ATHTTT, TTHTQT;
- 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**  
**TÌNH HÌNH 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 An toàn thông tin)

**1. Danh sách Bộ/Ngành**

TT	Bộ/Cơ quan ngang Bộ/ Cơ quan trực thuộc Chính phủ	SL máy chia sẻ dữ liệu trong tháng 7/2022	Ghi chú
1	Bộ Công Thương	1	
2	<b>Bộ Giáo dục và Đào tạo</b>	0	Chưa kết nối
3	Bộ Giao thông vận tải	0	Có kết nối nhưng chia sẻ thông tin không đầy đủ
4	Bộ Kế hoạch và Đầu tư	219	
5	Bộ Khoa học và Công nghệ	414	
6	<b>Bộ Lao động - Thương Binh và Xã hội</b>	0	Chưa kết nối
7	Bộ Ngoại giao	19	
8	Bộ Nội vụ	37	
9	<b>Bộ Nông nghiệp và Phát triển nông thôn</b>	0	Chưa kết nối
10	Bộ Tài chính	239	
11	Bộ Tài nguyên và Môi trường	175	
12	Bộ Tư pháp	461	
13	Bộ Văn hóa, Thể thao và Du lịch	59	
14	<b>Bộ Xây Dựng</b>	0	Mất kết nối 01 tháng trở lên
15	<b>Bộ Y tế</b>	0	Mất kết nối 01 tháng trở lên

16	Ngân hàng Nhà nước Việt Nam	0	Có kết nối nhưng chia sẻ thông tin không đầy đủ
17	Thanh tra Chính phủ	377	
18	<b>Ủy ban Dân tộc</b>	0	Chưa kết nối
19	<b>Văn phòng Chính phủ</b>	0	Mất kết nối 01 tháng trở lên
20	Ban Quản lý Lăng Chủ tịch HCM	14	
21	Đài Tiếng nói Việt Nam	30	
22	<b>Đài Truyền hình Việt Nam</b>	0	Mất kết nối 01 tháng trở lên
23	Viện Hàn lâm Khoa học Công nghệ	30	
24	<b>Thông tấn xã Việt Nam</b>	0	Mất kết nối 01 tháng trở lên
25	<b>Viện Hàn lâm Khoa học Xã hội</b>	0	Chưa kết nối

## 2. Danh sách Tỉnh/Thành

TT	Tỉnh/Thành	SL máy chia sẻ dữ liệu trong tháng 7/2022	Ghi chú
1	An Giang	0	Có kết nối nhưng chia sẻ thông tin không đầy đủ
2	Bắc Giang	655	
3	Bắc Kạn	0	Có kết nối nhưng chia sẻ thông tin không đầy đủ
4	Bạc Liêu	145	
5	Bắc Ninh	1291	
6	Bà Rịa - Vũng Tàu	0	Có kết nối nhưng chia sẻ thông tin không đầy đủ
7	Bến Tre	0	Có kết nối nhưng chia sẻ thông tin không đầy đủ



8	Bình Định	1	
9	<b>Bình Dương</b>	0	Chưa kết nối
10	Bình Phước	2012	
11	Bình Thuận	20	
12	Cà Mau	1027	
13	Cần Thơ	23	
14	<b>Cao Bằng</b>	0	Mất kết nối 01 tháng trở lên
15	Đắk Lắk	2710	
16	Đắk Nông	961	
17	Đà Nẵng	2901	
18	Điện Biên	2231	
19	Đồng Nai	48	
20	Đồng Tháp	1583	
21	Gia Lai	17	
22	Hà Giang	0	Có kết nối nhưng chia sẻ thông tin không đầy đủ
23	Hải Dương	2016	
24	<b>Hải Phòng</b>	0	Mất kết nối 01 tháng trở lên
25	Hà Nam	184	

26	Hà Nội	480	
27	Hà Tĩnh	1131	
28	Hòa Bình	3581	
29	Hồ Chí Minh	70	
30	<b>Hậu Giang</b>	0	Mất kết nối 01 tháng trở lên
31	Hung Yên	603	
32	Khánh Hòa	0	Có kết nối nhưng chia sẻ thông tin không đầy đủ
33	Kiên Giang	1233	
34	<b>Kon Tum</b>	0	Mất kết nối 01 tháng trở lên
35	Lai Châu	28	
36	Lâm Đồng	2372	
37	Lạng Sơn	1951	
38	Lào Cai	0	Có kết nối nhưng chia sẻ thông tin không đầy đủ
39	Long An	2967	
40	Nam Định	40	
41	Nghệ An	1365	
42	Ninh Bình	129	
43	Ninh Thuận	0	Có kết nối nhưng chia sẻ thông tin không đầy đủ

44	Phú Thọ	52	
45	<b>Phú Yên</b>	0	Mất kết nối 01 tháng trở lên
46	Quảng Bình	2	
47	Quảng Nam	94	
48	Quảng Ngãi	2158	
49	Quảng Ninh	1	
50	Quảng Trị	513	
51	Sóc Trăng	92	
52	Sơn La	1263	
53	Tây Ninh	2122	
54	Thái Bình	3122	
55	Thái Nguyên	55	
56	Thanh Hóa	2367	
57	Thừa Thiên Huế	1964	
58	Tiền Giang	1860	
59	Trà Vinh	70	
60	Tuyên Quang	0	Có kết nối nhưng chia sẻ thông tin không đầy đủ
61	Vĩnh Long	1951	

62	Vĩnh Phúc	1532	
63	Yên Bái	2689	

**Ghi chú:** - Một số đơn vị có số lượng máy chia sẻ dữ liệu trong tháng bằng 0, do đã có kết nối chia sẻ dữ liệu về NCSC tuy nhiên thông tin chia sẻ không đầy đủ. NCSC khuyến nghị các đơn vị kiểm tra lại quá trình chia sẻ kết nối, khắc phục tình trạng hiện tại.

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

**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**

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

20	Đài Truyền hình Việt Nam	14/9/2020	31/7/2022
21	Viện Hàn Lâm KHCN	22/9/2020	31/7/2022
22	Kiểm toán Nhà nước Việt Nam	09/3/2021	14/4/2022

## 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 31/7/2022)
1	An Giang	30/9/2020	24/7/2022
2	Bắc Giang	21/8/2020	02/6/2022
3	Bắc Kạn	01/9/2020	31/7/2022
4	Bạc Liêu	09/10/2020	31/7/2022
5	Bắc Ninh	23/7/2020	31/7/2022
6	Bà Rịa - Vũng Tàu	20/7/2020	31/7/2022
7	Bến Tre	10/8/2020	31/7/2022
8	Bình Định	05/6/2020	30/7/2022
9	Bình Dương	24/4/2020	02/7/2020
10	Bình Phước	23/4/2020	31/7/2022
11	Bình Thuận	31/8/2020	31/7/2022
12	Cà Mau	15/5/2020	31/7/2022
13	Cần Thơ	13/4/2020	31/7/2022
14	Cao Bằng	14/8/2020	31/7/2022
15	Đắk Lắk	17/6/2020	31/7/2022
16	Đắk Nông	31/8/2020	31/7/2022
17	Đà Nẵng	09/6/2020	31/7/2022
18	Điện Biên	02/6/2020	31/7/2022
19	Đồng Nai	15/6/2020	31/7/2022
20	Đồng Tháp	14/7/2020	24/7/2022
21	Gia Lai	14/9/2020	31/7/2022
22	Hà Giang	18/8/2020	24/7/2022

23	Hải Dương	04/9/2020	12/5/2022
24	Hải Phòng	28/7/2020	28/7/2022
25	Hà Nam	22/9/2020	31/7/2022
26	Hà Nội	30/6/2020	27/4/2022
27	Hà Tĩnh	06/10/2020	29/7/2022
28	Hòa Bình	13/5/2020	25/7/2022
29	Hồ Chí Minh	26/6/2020	31/7/2022
30	Hậu Giang	02/10/2020	24/7/2022
31	Hưng Yên	22/5/2020	29/7/2022
32	Khánh Hòa	21/9/2020	31/7/2022
33	Kiên Giang	24/9/2020	31/7/2022
34	Kon Tum	28/9/2020	31/7/2022
35	Lai Châu	26/9/2020	31/7/2022
36	Lâm Đồng	22/10/2020	17/3/2022
37	Lạng Sơn	08/10/2020	31/7/2022
38	Lào Cai	09/7/2020	31/7/2022
39	Long An	22/7/2020	31/7/2022
40	Nam Định	21/9/2020	31/7/2022
41	Nghệ An	09/9/2020	26/7/2022
42	Ninh Bình	28/7/2020	24/7/2022
43	Ninh Thuận	01/9/2020	31/7/2022
44	Phú Thọ	01/10/2020	31/7/2022
45	Phú Yên	30/11/2020	31/7/2022
46	Quảng Bình	01/7/2020	31/7/2022
47	Quảng Nam	14/9/2020	31/7/2022
48	Quảng Ngãi	12/8/2020	30/6/2022
49	Quảng Ninh	12/9/2020	18/3/2022
50	Quảng Trị	24/12/2020	14/7/2022
51	Sóc Trăng	12/8/2020	31/7/2022
52	Sơn La	13/7/2020	28/6/2021

53	Tây Ninh	08/7/2020	31/7/2022
54	Thái Bình	25/6/2020	05/7/2022
55	Thái Nguyên	19/11/2020	31/7/2022
56	Thanh Hóa	29/9/2020	02/6/2022
57	Thừa Thiên Huế	29/7/2020	31/7/2022
58	Tiền Giang	24/9/2020	31/7/2022
59	Trà Vinh	29/7/2020	31/7/2022
60	Tuyên Quang	19/11/2020	19/5/2022
61	Vĩnh Long	25/6/2020	21/7/2022
62	Vĩnh Phúc	30/6/2020	31/7/2022
63	Yên Bái	26/8/2020	29/7/2022



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

**1. Danh sách Bộ/Ngành**

TT	Tên đơn vị	Số lượng IP botnet tháng 6/2022	Số lượng IP botnet tháng 7/2022	Loại mã độc/botnet
1	Đài Tiếng nói Việt Nam	9	6	
2	Bộ Khoa học và Công nghệ	7	6	Avalanche
3	Kiểm toán Nhà nước	2	1	Avalanche
4	Bộ Tư Pháp	1	1	Avalanche
5	Viện Hàn lâm Khoa học và Công nghệ VN	2	1	
6	Bộ Kế hoạch và Đầu tư	0	1	

**2. Danh sách Tỉnh/thành**

TT	Tên đơn vị	Số lượng IP botnet tháng 6/2022	Số lượng IP botnet tháng 7/2022	Loại mã độc/botnet
1	Lai Châu	28	22	Lethic, Avalanche, Conficker
2	Thanh Hóa	14	12	Avalanche
3	Hà Nội	15	11	Lethic, Avalanche
4	Lâm Đồng	16	11	Avalanche

5	Long An	8	6	Lethic,
6	Lạng Sơn	11	4	Lethic, Necurs, Avalanche
7	Điện Biên	9	8	Lethic, Avalanche
8	Nam Định	12	9	Avalanche
9	Hà Nam	10	8	Wannacry, Lethic, Avalanche
10	Nghệ An	2	0	Lethic, Wannacry, Other, Avalanche
11	Đồng Tháp	5	4	Avalanche
12	Gia Lai	6	4	Avalanche
13	Bình Thuận	3	2	Necurs, Stealrat, Avalanche
14	Ninh Bình	6	2	Avalanche, Wannacry
15	Lào Cai	6	7	Avalanche
16	Quảng Ninh	6	5	Avalanche, Lethic
17	Hung Yên	2	2	Other, Wannacry, Lethic, Avalanche
18	Hải Phòng	6	3	Wannacry, Stealrat, Other, Avalanche
19	Thái Bình	6	4	Avalanche

20	Đắk Nông	7	7	Avalanche, Other
21	Bà Rịa Vũng Tàu	3	2	
22	Tuyên Quang	3	2	Avalanche, Conficker
23	Đắk Lắk	2	2	
24	Cao Bằng	2	1	
25	Cần Thơ	7	3	Wannacry, Lethic, Avalanche
26	Hà Tĩnh	4	1	Wannacry, Lethic, Avalanche
27	Bình Dương	3	2	Lethic, Emotet, Necurs, Avalanche
28	Quảng Trị	1	1	Avalanche
29	Bến Tre	1	1	Avalanche
30	Hòa Bình	1	0	
31	Kon Tum	3	0	
32	Yên Bái	1	0	Lethic, Avalanche
33	Vĩnh Phúc	2	1	Avalanche
34	An Giang	4	3	Avalanche
35	Hà Giang	9	6	Lethic, Avalanche
36	Đồng Nai	1	0	

37	Bắc Kạn	2	1	
38	Vĩnh Long	2	0	
39	Sơn La	1	0	

**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	<a href="http://skhcn.kontum.gov.vn/1.php">http://skhcn.kontum.gov.vn/1.php</a>	Sở Thông tin và Truyền thông Kon Tum				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 ĐIỂM YẾU LỖ HỒNG PHỔ BIẾN**  
**ĐÃ CÓ HƯỚNG DẪN KỸ THUẬT**

<b>TT</b>	<b>Mã điểm yếu/ lỗ hổng</b>	<b>Ghi chú</b>
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 <b>Sandworm APT</b>
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 <b>Moonsoon APT</b>
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 <b>APT 31</b>

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 <b>Silence APT</b>
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