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: 18 /BC-CATTT

Hà Nội, ngày 21 tháng 09 năm 2023

BÁO CÁO KỸ THUẬT
Tình hình an toàn thông tin tháng 08/2023 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

Microsoft

Văn bản số 1500/CATTT-NCSC về việc lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 08/2023 phát hàng ngày 21/8/2023.

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 **14** 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/

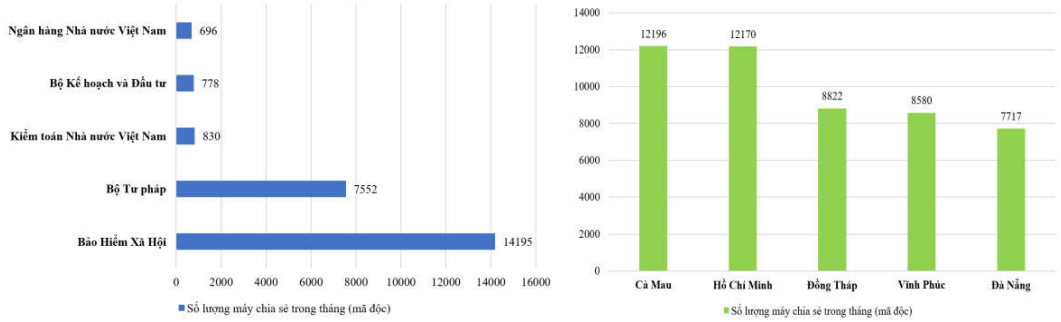
Đến hết tháng **08/2023** đã có **88** đơn vị (63 Tỉnh/Thành, 25 Bộ/Ngành) triển khai giải pháp phòng chống mã độc tập trung và thực hiện kết nối chia sẻ thông tin về mã độc với Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC).

Trong tháng **08/2023,** 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 **80/88** đơn vị có kết nối thường xuyên. Trong các đơn

vị kết nối thường xuyên có **80/80** đơn vị chia sẻ về hệ điều hành các máy (tổng số máy là **139.142**).

Tính đến tháng 08/2023 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.*

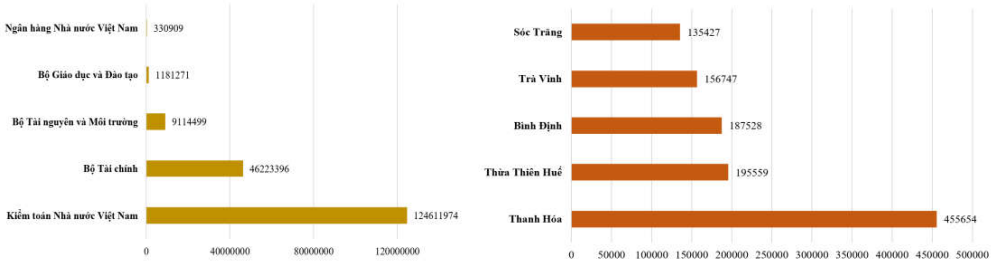
3. Tình hình triển khai công tác giám sát an toàn thông tin và kết nối chia sẻ dữ liệu giám sát theo Chỉ thị 14/CT-TTg năm 2019

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 **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 **08/2023** 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 **08/2023**, 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 **72/87** đơn vị có kết nối chia sẻ dữ liệu tương đối đầy đủ, **15/87** đơn vị bị mất kết nối chia sẻ dữ liệu.

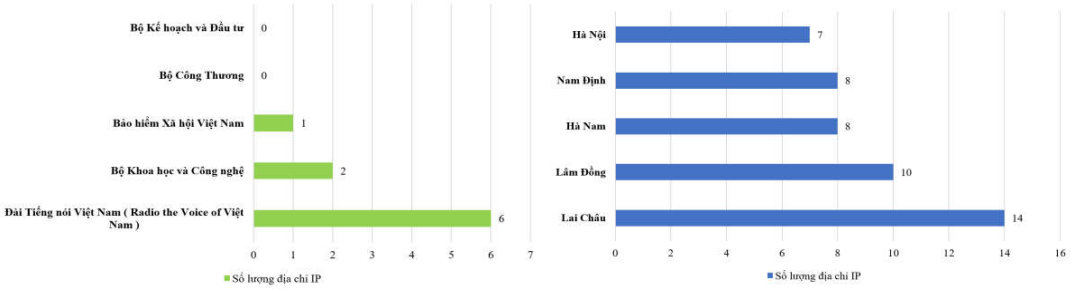
Một số đơn vị có kết nối chia sẻ dữ liệu giám sát trong tháng tương đối đầy đủ:



***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 **427.635** địa chỉ IP của Việt Nam nằm trong mạng botnet (giảm 3,9% so với tháng 07/2023), trong đó có 126 địa chỉ IP của cơ quan, tổ chức nhà nước (09 địa chỉ IP Bộ/Ngành, 117 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. Rà soát nội dung quảng cáo không phù hợp trên website của cơ quan nhà nước (.gov.vn)

Trong thời gian vừa qua, có rất nhiều website của cơ quan nhà nước bị lợi dụng để cài cắm, đăng tải, chuyển hướng hoặc liên kết với nội dung quảng cáo không phù hợp như: game bài, cờ bạc….

Ngày 19/12/2022, Bộ Thông tin và Truyền thông đã phát hành cảnh báo số 6327/BTTT-CATTTT về việc rà soát nội dung không phù hợp trên website của cơ quan nhà nước (.gov.vn).

Cục An toàn thông tin phát hành cảnh báo diện rộng số 381/CATTT-NCSC ngày 17/3/2023 và cảnh báo diện rộng số 972/CATTT-NCSC ngày 19/6/2023 về việc rà soát nội dung không phù hợp trên website của cơ quan nhà nước (.gov.vn).

Tuy nhiên đến thời điểm hiện tại, Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC) tiếp tục ghi nhận có **15** đơn vị (10 Tỉnh/Thành, 05 Bộ/Ngành) còn tồn tại các website của đơn vị bị lợi dụng để tải lên số lượng lớn tệp tin có nội dung độc hại. Những tệp tin này xuất hiện trong kết quả tìm kiếm của Google và thực hiện chuyển hướng người dùng sang website khác khi người dùng truy cập đường dẫn. Điều này sẽ trở nên nguy hiểm và nghiêm trọng nếu bị lợi dụng để đăng tải, phát tán những nội dung xấu độc, xuyên tạc về chủ quyền, chủ trương của Đảng và chính sách, pháp luật của Nhà nước.

Ghi chú: *Danh sách các đơn vị tồn tại các website chứa nội dung quảng cáo không phù hợp tại Phụ lục IV kèm theo.*

6. 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-UBQGCĐS 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-UBQGCĐS 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 **08/2023** đã có **79** đơn vị (58 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 **3255** website (547 website của 21 Bộ/Ngành, 2708 website của 58 Tỉnh/Thành).

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

7. 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 **63.595** 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	12276	https://nvd.nist.gov/vuln/detail/cve-2022-26809
2	CVE-2023-4078	6612	https://nvd.nist.gov/vuln/detail/CVE-2023-4078
3	CVE-2023-40477	6458	https://nvd.nist.gov/vuln/detail/CVE-2023-40477
4	CVE-2023-4368	4987	https://nvd.nist.gov/vuln/detail/CVE-2023-4368
5	CVE-2023-3740	4840	https://nvd.nist.gov/vuln/detail/CVE-2023-3740

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 2 kết nối nghi ngờ phát sinh trong tháng:

STT	IP/Domain nghi ngờ	STT	IP/Domain nghi ngờ

1	disorderstatus[.]ru	2	differentia[.]ru

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:
- Thứ trưởng Nguyễn Huy Dũng (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;
- Phòng ATHTTT, Phòng TT&HTQT, Trung tâm VNCERT/CC;
- Lưu: VT, NCSC.LTQ.

KT. CỤC TRƯỞNG
PHÓ CỤC TRƯỞNG

CỘNG HÒA X.H.C.N VIỆT NAM
CỤC AN TOÀN THÔNG TIN
BỘ THÔNG TIN VÀ TRUYỀN THÔNG

Trần Đăng Khoa

Phụ lục V

TÌNH HÌNH TRIỂN KHAI DÁN NHÃN TÍN NHIỆM MẠNG TRÊN CÁC TRANG, CỔNG THÔNG TIN ĐIỆN TỬ CỦA CƠ QUAN NHÀ NƯỚC

(Kèm theo Báo cáo số /BC-CATTT ngày tháng năm 2023 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 08/2023	Ghi chú
1	Bộ Ngoại giao	96	
2	Bộ Nội vụ	10	
3	Bộ Tư pháp	55	
4	Bộ Kế hoạch và Đầu tư	1	
5	Bộ Tài chính	130	
6	Bộ Công Thương	13	
7	Bộ Nông nghiệp và Phát triển nông thôn	11	
8	Bộ Giao thông vận tải	6	
9	**Bộ Xây dựng**	**0**	**Chưa đăng ký**
10	**Bộ Tài nguyên và Môi trường**	**0**	**Chưa đăng ký**
11	Bộ Thông tin và Truyền thông	16	
12	Bộ Lao động - Thương binh và Xã hội	1	
13	Bộ Văn hóa, Thể thao và Du lịch	1	
14	Bộ Khoa học và Công nghệ	14	
15	Bộ Giáo dục và Đào tạo	7	
16	Bộ Y tế	11	

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

2. Danh sách Tỉnh/Thành

TT	Tỉnh/Thành	Số lượng website được cấp nhãn đến tháng 08/2023	Ghi chú
1	An Giang	39	
2	Bà Rịa – Vũng Tàu	44	
3	Bắc Giang	37	
4	Bắc Kạn	48	
5	Bạc Liêu	5	
6	Bắc Ninh	64	
7	Bến Tre	36	
8	Bình Định	34	
9	Bình Dương	18	
10	Bình Phước	21	
11	Bình Thuận	34	
12	Cà Mau	41	
13	Cần Thơ	28	
14	Cao Bằng	36	
15	Đà Nẵng	79	
16	Đắk Lắk	6	

17	Đắk Nông	26	
18	Điện Biên	16	
19	Đồng Nai	2	
20	Đồng Tháp	65	
21	Gia Lai	30	
22	**Hà Giang**	**0**	**Chưa đăng ký**
23	Hà Nam	28	
24	Hà Nội	186	
25	**Hà Tĩnh**	**0**	**Chưa đăng ký**
26	Hải Dương	14	
27	Hải Phòng	4	
28	Hậu Giang	33	
29	Hòa Bình	28	
30	Hưng Yên	30	
31	Khánh Hòa	148	
32	Kiên Giang	70	
33	**Kon Tum**	**0**	**Chưa đăng ký**
34	Lai Châu	3	

35	Lâm Đồng	32	
36	Lạng Sơn	4	
37	Lào Cai	54	
38	Long An	47	
39	Nam Định	239	
40	Nghệ An	6	
41	Ninh Bình	23	
42	Ninh Thuận	30	
43	Phú Thọ	1	
44	Phú Yên	1	
45	Quảng Bình	33	
46	Quảng Nam	1	
47	Quảng Ngãi	78	
48	Quảng Ninh	27	
49	**Quảng Trị**	**0**	**Chưa đăng ký**
50	Sóc Trăng	65	
51	Sơn La	39	
52	Tây Ninh	45	

53	Thái Bình	26	
54	Thái Nguyên	1	
55	Thanh Hóa	62	
56	Thừa Thiên Huế	281	
57	Tiền Giang	31	
58	TP Hồ Chí Minh	8	
59	Trà Vinh	92	
60	**Tuyên Quang**	**0**	**Chưa đăng ký**
61	Vĩnh Long	147	
62	Vĩnh Phúc	45	
63	Yên Bái	37	