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: 12 /BC-CATTT

Hà Nội, ngày 21 tháng 06 năm 2023

BÁO CÁO KỸ THUẬT
Tình hình an toàn thông tin tháng 05/2023 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 729/CATTT-NCSC về việc lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 05/2023 phát hàng ngày 15/05/2023.

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

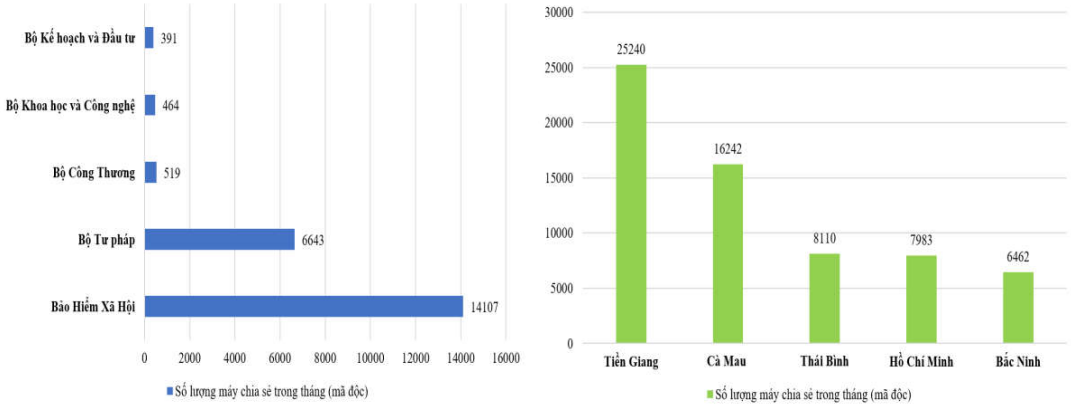
Thực hiện Chỉ thị số 14/CT-TTg của Thủ tướng Chính phủ ban hành ngày 25/5/2018 về việc nâng cao năng lực phòng, chống phần mềm độc hại, Cục An toàn thông tin đã giao Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC) hỗ trợ **14** doanh nghiệp có giải pháp phòng chống mã độc thực hiện kết nối 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://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 **05/2023** đã có **87** đơn vị (63 Tỉnh/Thành, 24 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 **05/2023,** thông qua kết nối chia sẻ dữ liệu về mã độc từ **87** đơn vị, Hệ thống kỹ thuật của Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC) ghi nhận **74/87** đơn vị có kết nối thường xuyên. Trong các đơn vị kết nối thường xuyên có **74/74** đơn vị chia sẻ về hệ điều hành các máy (tổng số máy là **148.834**).

Tính đến tháng 05/2023 có 04 đơn vị bao gồm: **Bộ Giáo dục và Đào tạo, Bộ Lao động - Thương Binh và Xã hội, 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

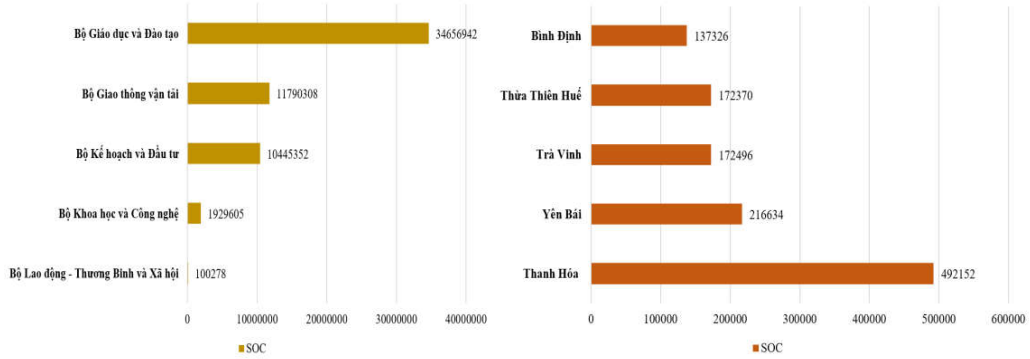
Thực hiện Chỉ thị số 14/CT-TTg của Thủ tướng Chính phủ ban hành ngày 07/6/2019 về việc tăng cường bảo đảm an toàn, an ninh mạng nhằm cải thiện chỉ số xếp hạng của Việt Nam, Cục An toàn thông tin đã giao Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC) hỗ trợ **13** doanh nghiệp có giải pháp 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 **05/2023** 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 **05/2023**, 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 **69/87** đơn vị có kết nối chia sẻ dữ liệu tương đối đầy đủ, **18/87** đơn vị bị mất kết nối chia sẻ dữ liệu.

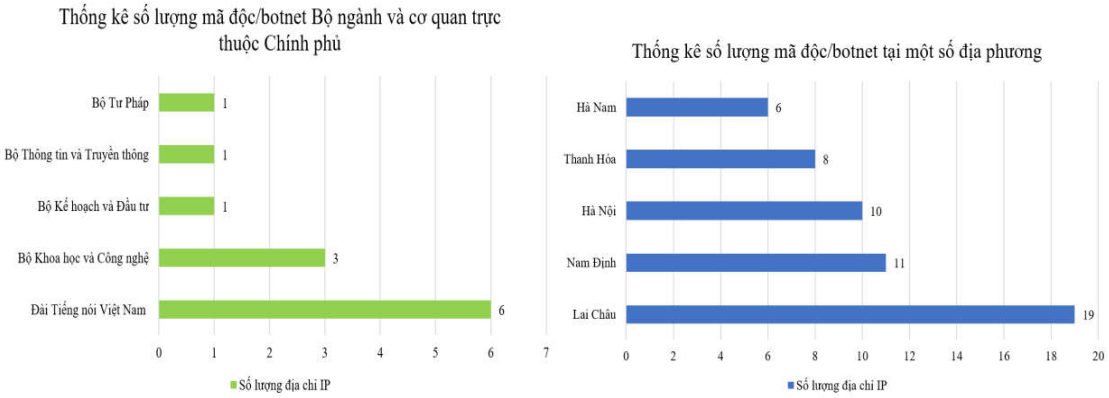
Một số đơn vị có kết nối chia sẻ dữ liệu giám sát trong tháng tương đối đầy đủ:



***Ghi chú**:* Hiện trạng kết nối chia sẻ dữ liệu giám sát tại Phụ lục 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 **512.712** địa chỉ IP của Việt Nam nằm trong mạng botnet (giảm 11% so với tháng 04/2023), trong đó có 160 địa chỉ IP của cơ quan, tổ chức nhà nước (13 địa chỉ IP Bộ/Ngành, 147 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 **58.100** 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	11682	https://nvd.nist.gov/vuln/detail/cve-2022-26809
2	CVE-2023-2468	10229	https://nvd.nist.gov/vuln/detail/CVE-2023-2468
3	CVE-2023-2726	6184	https://nvd.nist.gov/vuln/detail/CVE-2023-2726
4	CVE-2023-21716	4339	https://nvd.nist.gov/vuln/detail/CVE-2023-21716
5	CVE-2023-27366	3673	https://nvd.nist.gov/vuln/detail/CVE-2023-27366

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 4 kết nối nghi ngờ phát sinh trong tháng:

STT	IP/Domain nghi ngờ	STT	IP/Domain nghi ngờ
1	atomictrivia.ru	3	differentia.ru
2	disorderstatus.ru	4	103.200.97.189

Nhằm đảm bảo an toàn hệ thống, đề nghị đơn vị chuyên trách về CNTT/ATTT tại cơ quan, tổ chức rà soát xác định và tiến hành "Vá" các lỗi trên hệ thống, đặc biệt là các lỗ hổng, điểm yếu nêu trên.

Trân trọng./.

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;
- ATHTTT, TT&HTQT, VNCERT/CC;
- Lưu: VT, NCSC.

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