

Số: 9 /BC-CATT

Hà Nội, ngày 08 tháng 07 năm 2022

BÁO CÁO KỸ THUẬT

Tình hình an toàn thông tin tháng 6/2022
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 786/CATT-NCSC về việc lỗ hổng bảo mật CVE-2022-30190 trong Microsoft Support Diagnostic Tool phát hành ngày 01/6/2022.



Văn bản số 869/CATT-NCSC về việc lỗ hổng bảo mật ảnh hưởng Cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 6/2022.

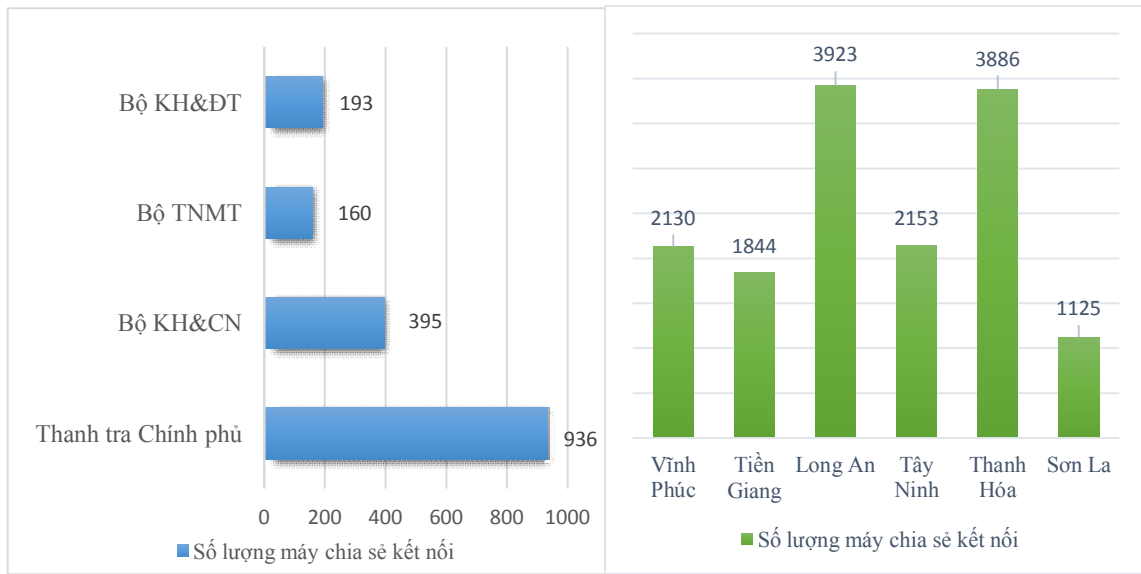
2. Tình hình triển khai công tác phòng chống phần mềm độc hại và chia sẻ dữ liệu mã độc theo Chỉ thị 14/CT-TTg năm 2018

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-CATT 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 6/2022 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 **6/2022**, 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 **72/83** đơn vị có kết nối thường xuyên, **54/72** đơn vị có chia sẻ về hệ điều hành các máy (tổng số máy là **68.977**).

Một số đơn vị có số lượng máy chia sẻ kết nối trong tháng 6 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

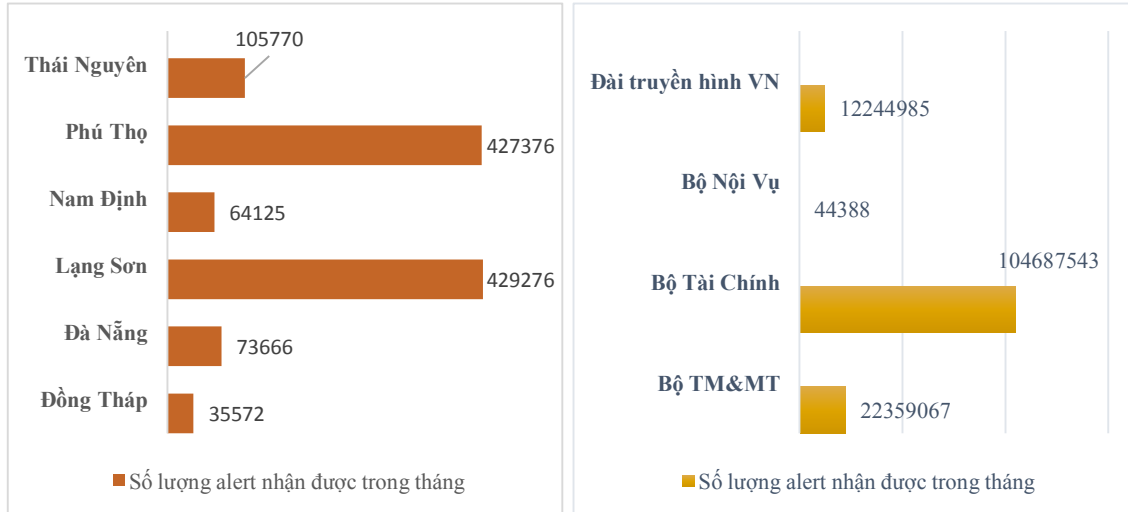
Thực hiện Chỉ thị số 14/CT-TTg của Thủ tướng Chính phủ ban hành ngày 07/6/2019 về việc tăng cường bảo đảm an toàn, an ninh mạng nhằm cải thiện chỉ số xếp hạng của Việt Nam, Cục An toàn thông tin đã giao Trung tâm Giám sát an toàn không gian mạng quốc gia hỗ trợ **13** doanh nghiệp có giải pháp giám sát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

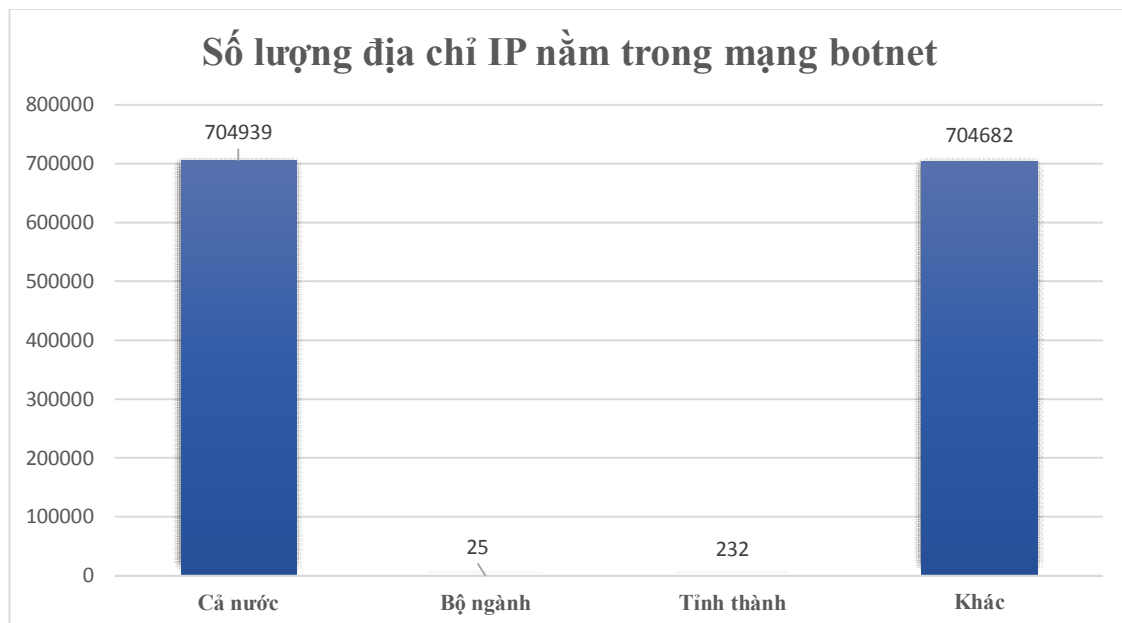
Một số đơn vị có kết nối chia sẻ dữ liệu giám sát trong tháng tương đối đầy đủ:

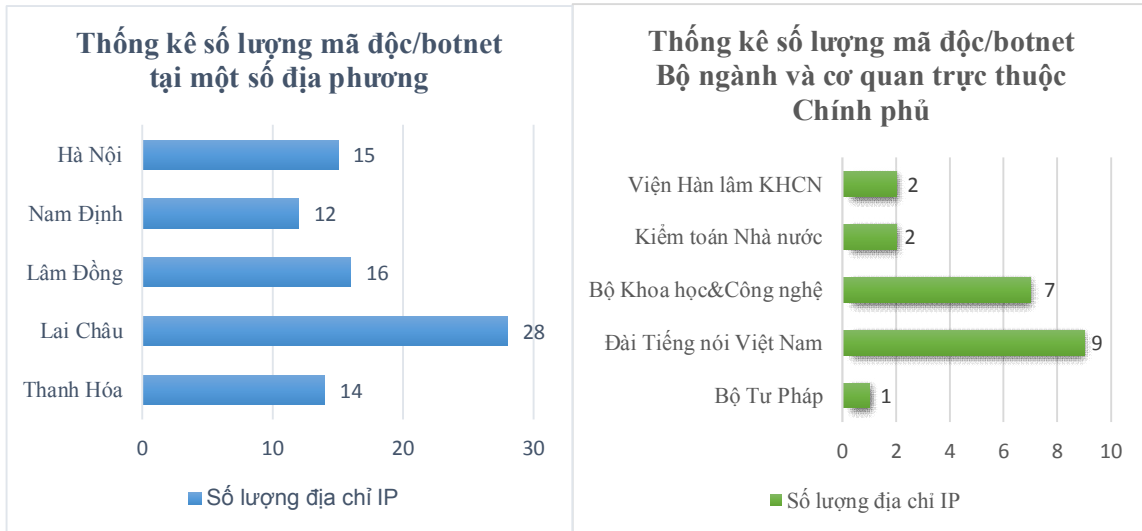


Ghi chú: Hiện trạng kết nối chia sẻ dữ liệu giám sát tại Phụ lục 2 kèm theo.

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 704,939 địa chỉ IP của Việt Nam nằm trong mạng botnet, trong đó có 257 địa chỉ IP của cơ quan, tổ chức nhà nước (25 địa chỉ IP Bộ/Ngành, 232 địa chỉ IP Tỉnh/Thành) giảm 5,38% so với tháng 5/2022.





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 **1.932** 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-2019-5126	1626	https://www.rapid7.com/db/vulnerabilities/foxit_reader-cve-2019-5126/

2	CVE-2020-13547	1508	https://talosintelligence.com/vulnerability_reports/TALOS-2020-1165
3	CVE-2018-20250	1319	https://nvd.nist.gov/vuln/detail/cve-2018-20250
4	CVE-2018-11617	1183	https://www.foxit.com/support/security-bulletins.html
5	CVE-2017-11209	1156	https://helpx.adobe.com/security/products/acrobat/apsb17-24.html

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	9	atomictrivia.ru
2	ugroocuw.net	10	d24ak3f2b.top
3	coinhive.com	11	d3g5ovfngjw9bw.cloudfront.net
4	pu-file.com	12	freeprosoftz.com
5	lookujie.net	13	marketwantocean.buzz
6	xtgem.com	14	trustiseverything.de
7	thedarkprice.xyz	15	rtbxheartbid.com

8	donttbeevils.de	16	zxb.isdun.com
---	-----------------	----	---------------

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 V
DANH SÁCH ĐIỂM YẾU LỖ HỒNG PHỔ BIẾN
ĐÃ CÓ HƯỚNG DẪN KỸ THUẬT

TT	Mã điểm yếu/ lỗ hồng	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