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

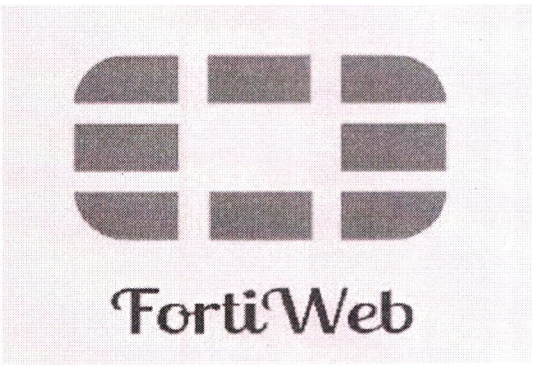
Số: 13 /BC-CATTT

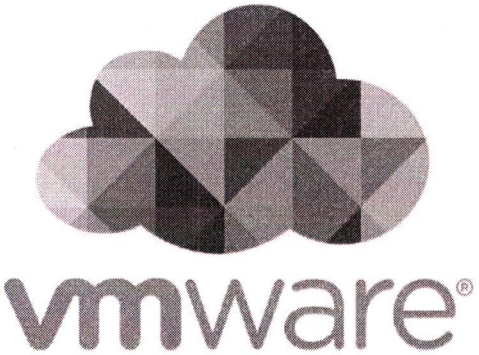
Hà Nội, ngày 11 tháng 6 năm 2021

BÁO CÁO KỸ THUẬT
Tình hình an toàn thông tin tháng 05/2021 và thống kê kết nối chia sẻ thông tin về mã độc

1. Thông tin cảnh báo về các lỗ hổng bảo mật trong tháng

Cảnh báo số 58/NCSC-ĐTPT ngày 03 tháng 06 năm 2021 về việc cảnh báo lỗ hổng bảo mật mới trong FortiWeb.



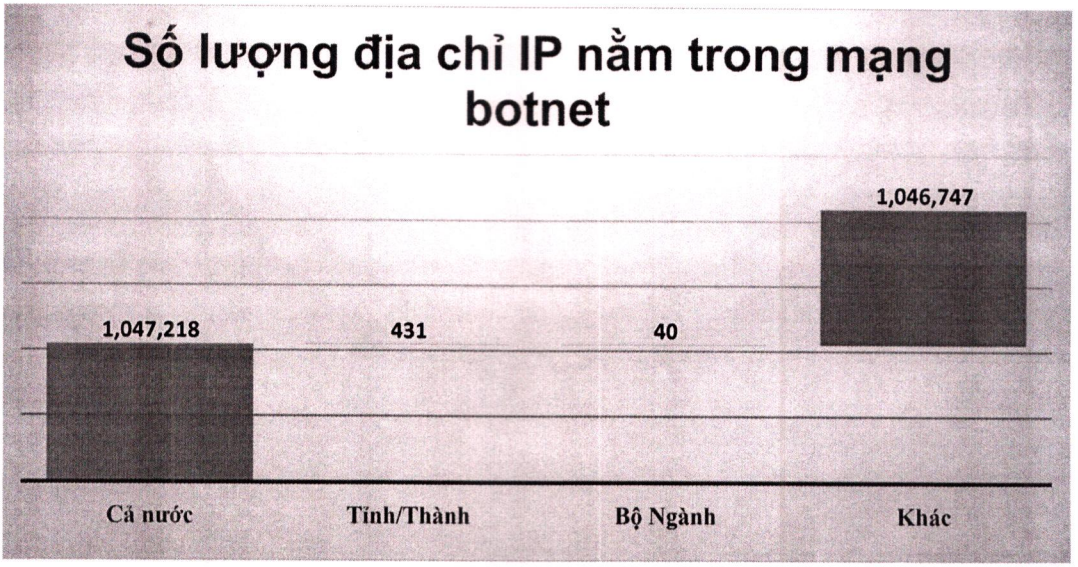


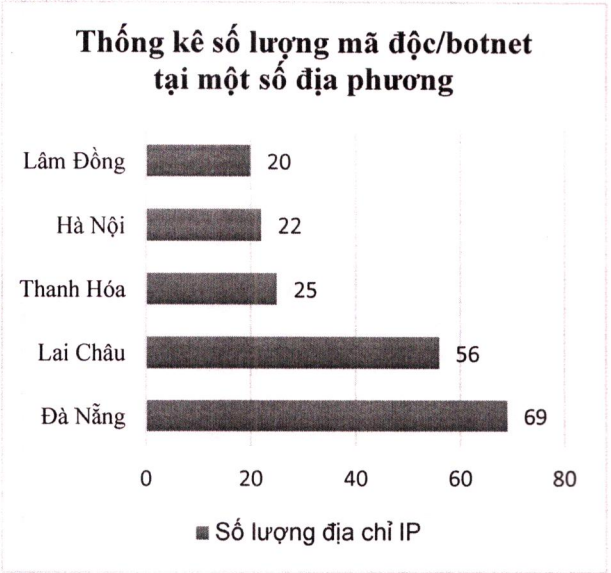
Ngày 26 tháng 5 năm 2021, Trung tâm NCSC đã có cảnh báo qua email đến các cơ quan tổ chức về lỗ hổng bảo mật mới (CVE-2021-21985, CVE-2021-21986) trong Vmware vCenter Server.

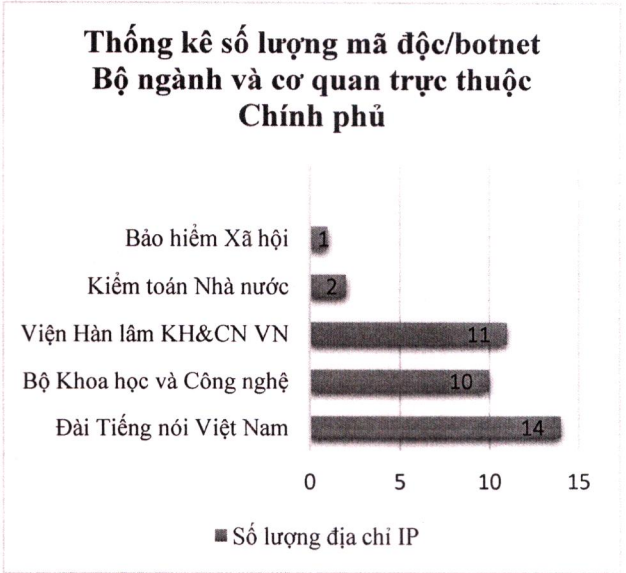
2. Tình hình lây nhiễm mã độc trên cả nước

Trong tháng, Hệ thống kỹ thuật của Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC) đã ghi nhận 1.047.218 địa chỉ IP của Việt Nam nằm trong mạng botnet, trong đó có 471 địa chỉ IP của cơ quan, tổ chức nhà nước (40 địa chỉ IP Bộ/Ngành, 431 địa chỉ IP Tỉnh/Thành) tăng 6.66% so với tháng 04/2021.

Danh sách các đơn vị có địa chỉ IP nằm trong mạng botnet mà Trung tâm NCSC phát hiện có tại phụ lục 3 kèm theo.





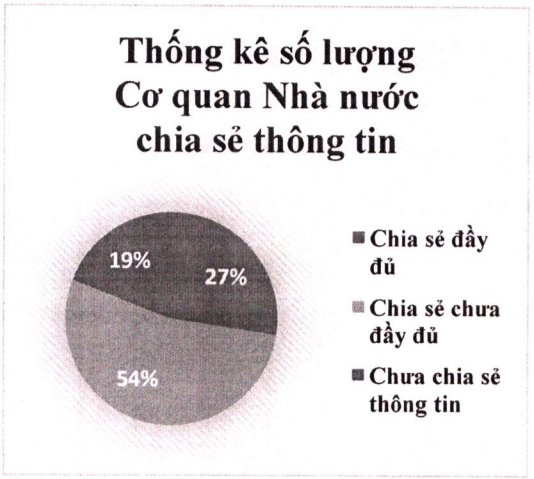


Thông tin chi tiết về các địa chỉ IP nằm trong mạng botnet đơn vị chuyên trách về CNTT/ATTT tại Bộ/Ngành, Tỉnh/Thành có thể tra cứu, cập nhật thông tin thường xuyên thông qua tài khoản đã có trên Hệ thống giám sát từ xa do Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC) cấp. Thông tin từ Hệ 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.

3. Tình hình chia sẻ dữ liệu theo Chỉ thị 14/CT-TTg 2018

Bên cạnh việc giám sát từ xa dựa trên dải địa chỉ IP tĩnh do Bộ/Ngành, Tỉnh/Thành cung cấp, Cục ATTT hiện đã triển khai kết nối chia sẻ thông tin về mã độc theo chỉ đạo tại 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.

Đến hết tháng 05/20201 đã có 81 đơn vị (60 Tỉnh/Thành, 21 Bộ/Ngành) thực hiện kết nối chia sẻ thông tin về mã độc với Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC).



Ghi chú:

- Đây là số lượng thống kê của Cơ quan Nhà nước bao gồm cả cơ quan Bộ/Ngành và Tỉnh/Thành. Trong đó:

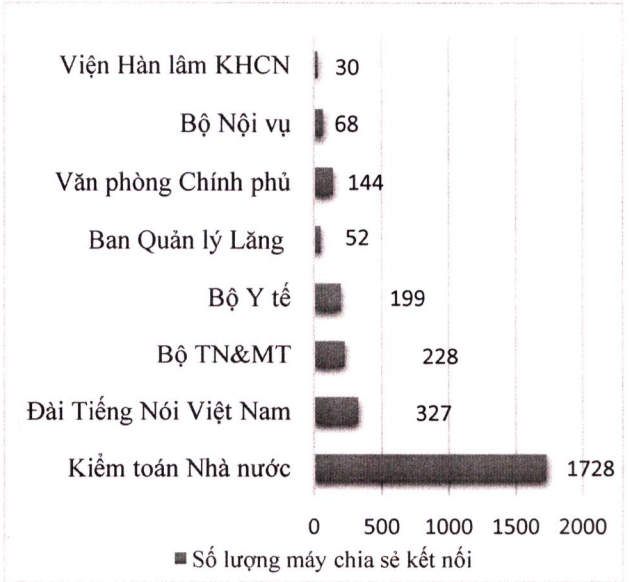
✓ Đã chia sẻ thông tin tương đối đầy đủ: 23 đơn vị (1 Bộ/Ngành, 22 Tỉnh/Thành)

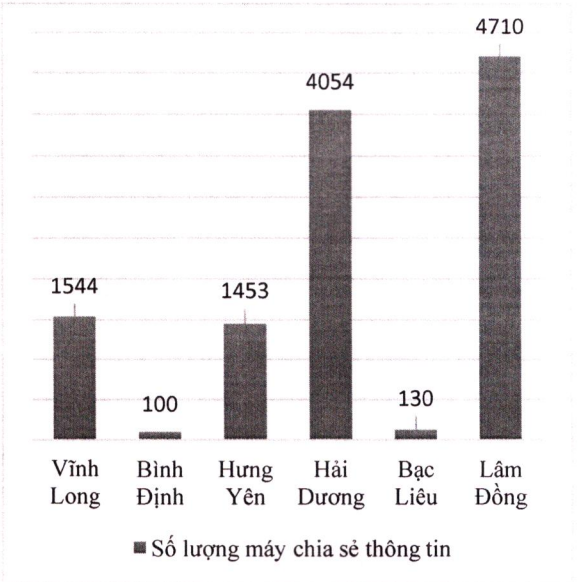
✓ Chia sẻ thông tin chưa đầy đủ: 46 đơn vị (16 Bộ/Ngành, 30 Tỉnh/Thành)

✓ Chưa chia sẻ thông tin: 15 đơn vị (11 Bộ/Ngành, 4 Tỉnh/Thành)

Một số đơn vị đang tích cực triển khai theo chỉ đạo của Thủ tướng Chính phủ gồm **Ban Quản lý Lăng Chủ tịch HCM, Bộ Xây dựng, Bộ Y tế, Thái Bình, Lào Cai, Long An, Nghệ An, Tây Ninh,...** Đây là những đơn vị triển khai chia sẻ dữ liệu tương đối tốt (có trên 50% các máy trên địa bàn đã được cài đặt giải pháp phòng chống mã độc và chia sẻ đầy đủ thông tin với Trung tâm Giám sát an toàn không gian mạng quốc gia).

Số lượng máy chia sẻ kết nối tháng 05:





4. Thông tin chung điểm yếu lỗ hổng

Trong tháng, Hệ thống kỹ thuật của NCSC đã ghi nhận có **1.538** điểm yếu, lỗ hổng an toàn thông tin tại các hệ thống thông tin của các cơ quan tổ chức nhà nước. Lỗ hổng gây mất an toàn thông tin tồn tại trên nhiều máy tính đã kết nối, chia sẻ thông tin.

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	Số lượng máy tồn tại lỗ hổng tháng 04	Số lượng máy tồn tại lỗ hổng tháng 05	Ghi chú
1	CVE-2020-1097	882	1.696	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2020-1097
2	CVE-2020-0655	846	1.636	https://msrc.microsoft.com/update-guide/en-us/vulnerability/CVE-2020-0655
3	CVE-2019-0708	689	1.312	Tham khảo Báo cáo tháng 9/2019
4	CVE-2015-0009 (MS15-014)	505	982	Tham khảo Báo cáo tháng 9/2019
5	CVE 2013-3900 (MS13-098)	481	921	Tham khảo Báo cáo tháng 8/2019

Nhằm đảm bảo an toàn hệ thống, đề nghị đơn vị chuyên trách về CNTT/ATTT tại cơ quan Nhà nước 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

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

Trần Quang Hưng

Phụ lục 1
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
(Chưa kết nối chia sẻ dữ liệu về Cục ATTTT)

1. Đối với Bộ/Ngành

TT	Bộ/Cơ quan ngang Bộ/ Cơ quan trực thuộc Chính phủ
1	Bộ Công Thương (đang kết nối)
2	Bộ Giáo dục và Đào tạo
3	Bộ LĐTB&XH
4	Bộ Nông nghiệp và Phát triển nông thôn
5	Ủy ban Dân tộc
6	Học viện Chính trị Quốc gia Hồ Chí Minh
7	Viện Hàn lâm Khoa học Xã hội

2. Đối với Tỉnh/Thành

TT	Tỉnh/Thành
1	Bình Dương
2	Quảng Nam
3	Yên Bái

Ghi chú: Thông tin về các Bộ/Ngành, Tỉnh/Thành chưa thực hiện kết nối chia sẻ thông tin về mã độc sẽ được Cục ATTT tổng hợp, báo cáo hàng tháng nhằm đôn đốc việc thực hiện chỉ tiêu mà Chính phủ đưa ra tại Nghị quyết 01/NQ-CP ngày 01/01/2020 của Chính phủ. Cụ thể: "90% các bộ, ngành, địa phương kết nối với Trung tâm Giám sát an toàn không gian mạng quốc gia".

Phụ lục 2

Danh sách điểm yếu lỗ hổng phổ biến đã có hướng dẫn kỹ thuật

STT	Mã điểm yếu/ lỗ hổng	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

Phụ lục 3

Danh sách các đơn vị phát hiện có địa chỉ IP nằm trong mạng botnet

1. Danh sách Tỉnh thành

TT	Tên đơn vị	Số lượng Ip botnet tháng 5	Loại mã độc/botnet
1	Đà Nẵng	69	Necurs, Wannacry, Gamut, Avanlanche, Conficker
2	Lai Châu	56	Other, Sality, Wannacry,Lethic, Confiker, Avalanche
3	Thanh Hóa	25	Other, Lethic, Necurs, Avalanche
4	Hà Nội	22	Lethic, Necurs, Stealrat, Wannacry, Avalanche
5	Lâm Đồng	20	Pykspa, Wannacry, Lethic, Other, Avalanche
6	Long An	17	Wannacry, Lethic, Other, Avalanche
7	Lạng Sơn	14	Other, Wannacry, Lethic, Necurs, Gamut, Conficker, Avalanche
8	Điện Biên	14	Sality, Conficker, Necurs, Avalanche
9	Nam Định	13	Wannacry, Lethic, Other, Conficker, Avalanche

10	Hà Nam	12	Wannacry, Lethic, Avalanche
11	Nghệ An	12	Lethic, Wannacry, Other, Avalanche
12	Đồng Tháp	12	Lethic, Wannacry, Other, Avalanche, Necurs, Pykspa
13	Gia Lai	11	Avalanche
14	Bình Thuận	10	Necurs, Stealrat, Avalanche
15	Ninh Bình	10	Avalanche, Wannacry
16	Hà Giang	9	Conficker, Lethic, Avalanche
17	Lào Cai	8	Lethic, Wanancry, Other, Pykspa, Stealrat, Avalanche
18	Quảng Ninh	8	Avalanche, Lethic
19	Hưng Yên	7	Other, Wannacry, Lethic, Avalanche
20	Hải Phòng	6	Wannacry, Stealrat, Other, Avalanche
21	Thái Bình	6	Avalanche
22	Đắk Nông	6	Avalanche, Other
23	An Giang	5	Avalanche

24	Bà Rịa Vũng Tàu	5	
25	Tiền Giang	5	Wannacry, Lethic, Avalanche
26	Tuyên Quang	5	Avalanche, Conficker
27	Đắk Lắk	5	
28	Cao Bằng	4	Avalanche
29	Cần Thơ	4	Wannacry, Lethic, Avalanche
30	Hà Tĩnh	4	Wannacry, Lethic, Avalanche
31	Vĩnh Phúc	4	Avalanche
32	Bình Dương	3	Lethic, Emotet, Necurs, Avalanche
33	Quảng Ngãi	3	Avalanche
34	Quảng Trị	3	Avalanche
35	Vĩnh Long	3	Avalanche
36	Bình Phước	2	Avalanche, Conficker
37	Bến Tre	2	Avalanche
38	Hòa Bình	2	Avalanche
39	Kon Tum	2	Avalanche, Wannacry

40	Bắc Kạn	1	Avalanche, Wannacry
41	Phú Thọ	1	
42	Yên Bái	1	Wannacry, Lethic, Other, Avalanche
43	Đồng Nai	1	Avalanche

2. Danh sách Bộ ngành

TT	Tên đơn vị	Số lượng IP botnet tháng 5	Loại mã độc/botnet
1	Đài Tiếng nói Việt Nam	14	Avalanche, Stealrat, Lethic, Conficker
2	Viện Hàn lâm khoa học và Công nghệ Việt Nam	56	Sality, Wannacry, Stealrat, Conficker, Avalanche
3	Bộ Khoa học và Công nghệ	25	Sality, Lethic, Stealrat, Necurs, Wannacry, Avalanche
4	Kiểm toán Nhà nước	22	Wannacry, Lethic, Avalanche
5	Bảo hiểm Xã hội Việt Nam	20	Necurs
6	Bộ Tư pháp	1	Avalanche
7	Văn phòng Quốc hội	1	Avalanche