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: /BC-CATTT

Hà Nội, ngày tháng năm 2021

BÁO CÁO KỸ THUẬT
Tình hình an toàn thông tin tháng 03/2021 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:

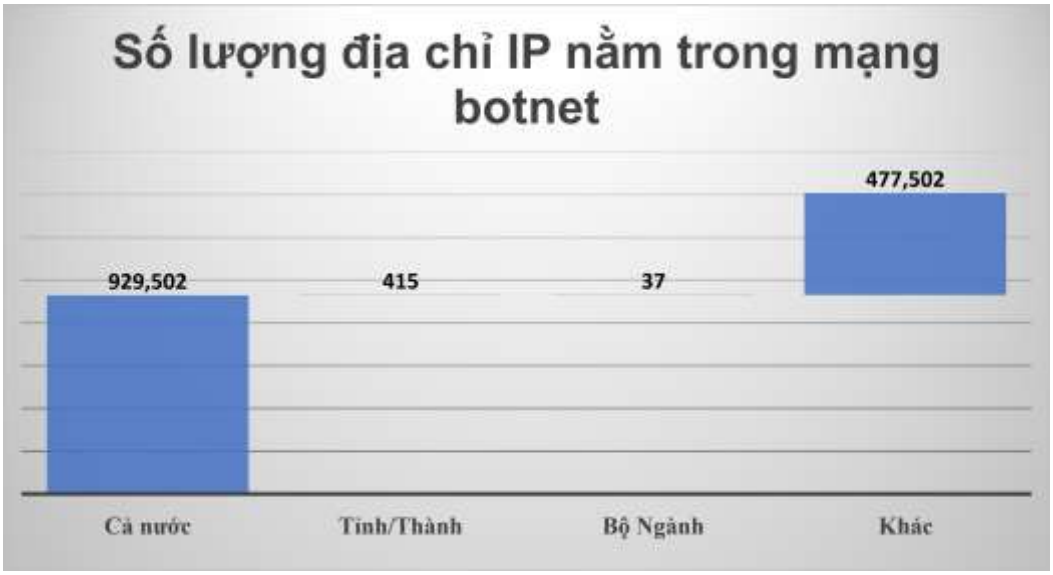
Cảnh báo số 13 /CATTT-NCSC ngày 03 tháng 03 năm 2021 về việc lỗ hổng bảo mật trong Microsoft Exchange Server.

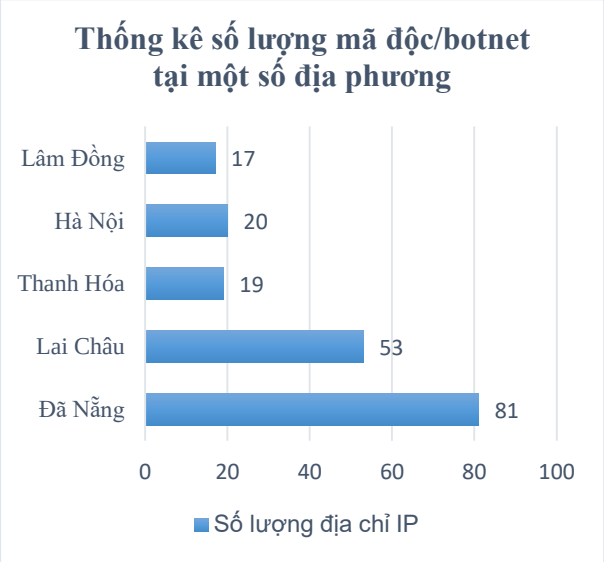
Cảnh báo số 14 /CATTT-NCSC ngày 11 tháng 03 năm 2021 về việc lỗ hổng bảo mật trong thiết bị F5 BIG-IP.

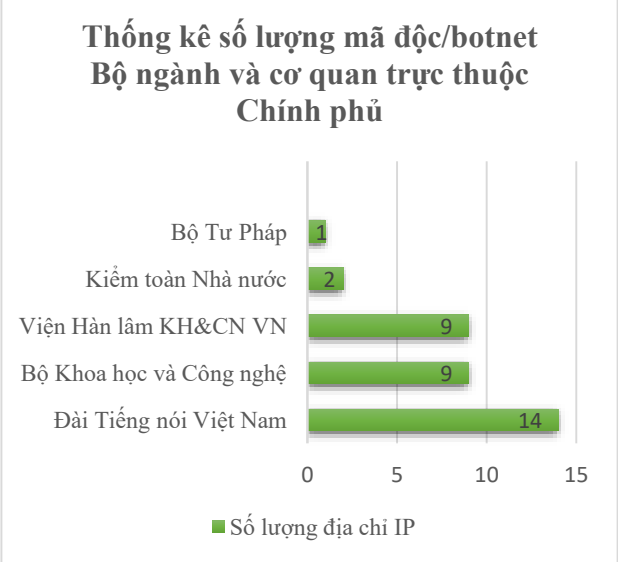
Cảnh báo số 44 /CATTT-NCSC ngày 31 tháng 03 năm 2021 về việc cảnh báo lỗ hổng bảo mật trong sản phẩm Vmware.

2. Tình hình lây nhiễm mã độc trên cả nước

Trong tháng, Hệ thống kiểm tra của Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC) đã ghi nhận 929.502 địa chỉ IP của Việt Nam nằm trong mạng botnet, trong đó có 452 địa chỉ IP của cơ quan, tổ chức nhà nước (37 địa chỉ IP Bộ/Ngành, 415 địa chỉ IP Tỉnh/Thành) giảm 4.65% so với tháng 02/2021.







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 giám sát từ Hệ thống 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 03/20201 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:

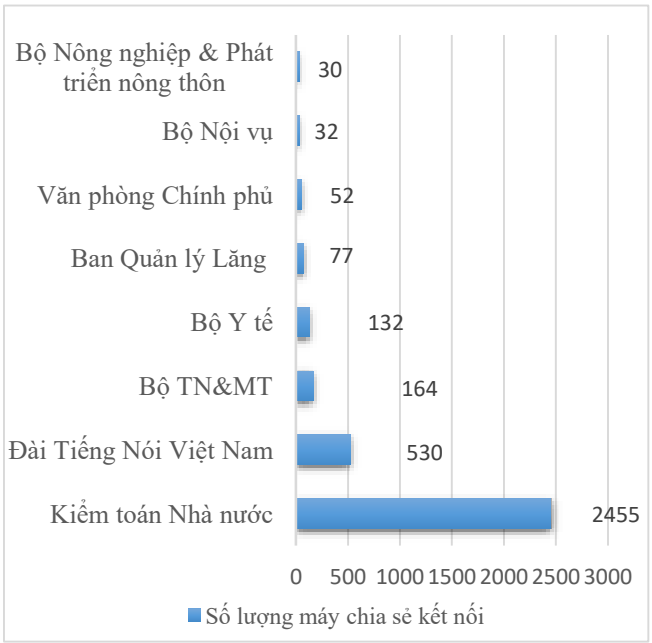
✓ Đã chia sẻ thông tin tương đối đầy đủ: 23 đơn vị (1 Bộ/Ngành, 22 Tỉnh/Thành)

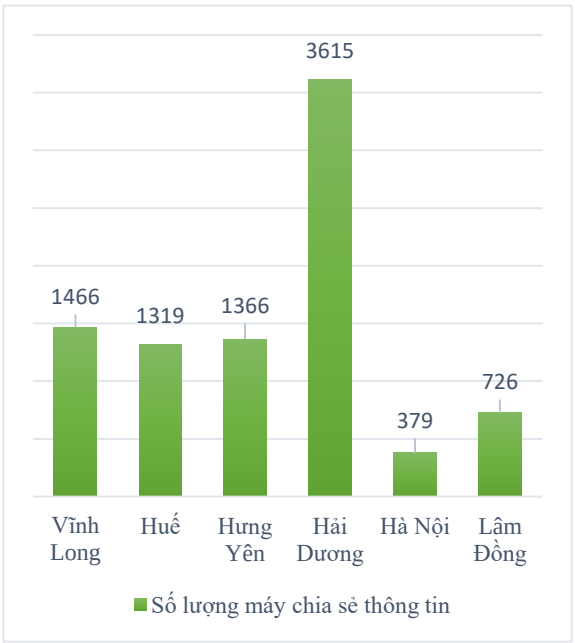
✓ Chia sẻ thông tin chưa đầy đủ: 46 đơn vị (16 Bộ/Ngành, 30 Tỉnh/Thành)

✓ 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 03:





4. Thông tin chung điểm yếu lỗ hổng

Trong tháng, Hệ thống kỹ thuật của NCSC đã ghi nhận có **1.608** 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 02	Số lượng máy tồn tại lỗ hổng tháng 03	Ghi chú
1	CVE-2020-1097	1.147	1.806	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2020-1097
2	CVE-2020-0655	1.116	1.765	https://msrc.microsoft.com/update-guide/en-us/vulnerability/CVE-2020-0655
3	CVE-2019-0708	962	1.444	Tham khảo Báo cáo tháng 9/2019
4	CVE-2015-0009 (MS15-014)	797	1.167	Tham khảo Báo cáo tháng 9/2019
5	CVE 2013-3900 (MS13-098)	798	1.167	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);
- PCT Nguyễn Khắc Lịch;
- Lưu: VT, NCSC.

KT. CỤC TRƯỞNG
PHÓ CỤC TRƯỞNG

Nguyễn Khắc Lịch

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
Thông tin về các loại mã độc/botnet

Tên gọi	Một số IP – Tên miền	Mô tả
Avalanche (Win32/Gamarue)	somicrososoft.ru morphed.ru a.deltaheavy.ru hzmksreiuojy.in devicesta.ru designthefuture.ru andall.andddddzandddd2.com ochengorit.ru and32.microscobisoftng5.com letstryitnowx.online cp.4jhlti79.ru cp.oa505txz.ru cp.qc0zt6eo.ru cp.4nbizac8.ru b.deltaheavy.ru c.deltaheavy.ru cp.x1yuqjh9.ru and19.themarket12345sushi3.com cp.ekic4bf5.ru	- Thời gian xuất hiện: Năm 2011. - Mục tiêu tấn công: Doanh nghiệp sử dụng thẻ thanh toán. - Các chức năng chính như: Keylogging; Rootkit; Truy cập từ xa ẩn; Thu thập thông tin đăng nhập từ trình duyệt. - Mục đích chính là phát tán các dòng mã độc khác nhằm phục vụ các cuộc tấn công phần mềm độc hại toàn cầu. Mạng botnet Andromeda bao gồm và có liên quan đến ít nhất 80 họ phần mềm độc hại, trong đó chủ yếu là họ mã độc Point of Sale (POS), ví dụ như GamaPOS.
SmokeLoader	173.231.184.57 173.231.184.5 206.189.61.126 ukcompany.me ukcompany.pw ukcompany.top	- Xuất hiện từ đầu tháng 01/2018, Meltdown và Specter là hai phương pháp tấn công qua kênh mới nhắm vào bộ vi xử lý hiện đại và được cho là ảnh hưởng đến hàng tỷ thiết bị. Đây là các lỗ hổng ở cấp CPU, cho phép các ứng dụng độc hại truy cập vào dữ liệu khi đang được xử lý, bao gồm mật khẩu, ảnh, tài liệu, email và những thứ tương tự. Mã độc Smoke Loader đặc biệt hoạt động mạnh trong suốt năm 2018 với nhiều chiến dịch phát tán Smoke Loader qua các bản vá lỗi giả mạo dành cho lỗ hổng Meltdown và Spectre.

Conficker	149.93.100.83 149.93.123.143 149.93.131.229 149.93.132.110 149.93.138.146 149.93.149.250 149.93.154.218 149.93.155.237 149.93.16.132 149.93.16.142 149.93.170.119 149.93.179.14 149.93.179.249 149.93.180.45 149.93.20.179 149.93.203.187	- Thời gian phát hiện: từ tháng 10/2008. - Lợi dụng lỗ hổng cũ (MS 08-067), đã có bản vá bảo mật. - Mục tiêu: Nhằm vào hệ điều hành Microsoft Windows. Khi mã độc này lây nhiễm vào một máy tính, thì máy tính này tham gia vào mạng botnet và có thể bị điều khiển để gửi thư rác (spam) và tấn công các hệ thống khác.
Sality (KuKu)	4b998.bmakemegood24.com axr.lukki6nd2kdnc.info bdd.f5ds1jkkk4d.info blog.inform1ongung.info businecessity.com dddrbcash.net dyfa.lukki6nd2kdnc.info gyi.f5ds1jkkk4d.info jcnqg.lukki6nd2kdnc.info jlw.lukki6nd2kdnc.info jwyo.f5ds1jkkk4d.info kukutrustnet666.info mdagk.f5ds1jkkk4d.info mim.lukki6nd2kdnc.info opxp.f5ds1jkkk4d.info qdxc.lukki6nd2kdnc.info rqkh.f5ds1jkkk4d.info rvj.lukki6nd2kdnc.info trfqi.f5ds1jkkk4d.info vawp.lukki6nd2kdnc.info	- Thời gian phát hiện: lần đầu tiên bị phát hiện vào 04/6/2003. - Tấn công vào các máy tính sử dụng hệ điều hành Windows, - Thời điểm Sality là một mã độc lây nhiễm vào hệ thống qua các đoạn mã chèn vào đầu tập tin host để mở cửa hậu và lấy trộm thông tin bàn phím. Đến năm 2010 xuất hiện biến thể Sality nguy hiểm hơn và trở thành một trong những dòng mã độc phức tạp và nguy hiểm nhất đối với an toàn của hệ thống. Máy tính bị nhiễm mã độc sẽ trở thành một điểm trong mạng ngang hàng để tiếp tục phát tán mã độc sang các máy tính khác. Sality chủ yếu để phát tán thư rác, tạo ra các proxy, ăn cắp thông tin cá nhân, lây nhiễm vào các máy chủ web để biến các máy chủ này

		thành máy chủ điều khiển của mạng botnet để tiếp tục mở rộng mạng botnet.
Lokibot		- Thời gian phát hiện: tháng 2 năm 2016. - Lokibot lợi dụng khai thác lỗ hổng CVE-2017-11882, CVE-2018-0802, CVE-2018-20250 - Mục tiêu: hệ điều hành Windows và Android nhằm thu thập thong tin mật khẩu người dùng, thông tin ngân hàng, máy tính của nạn nhân trở thành một bot trong mạng botnet. - Phương thức lây lan: Email đính kèm file chứa mã độc, quảng cáo trực tuyến độc hại,… - Phiên bản mới nhất của Lokibot có khả năng spammed ra cho các nạn nhân với số lượng lớn, và sử dụng một thủ thuật thông minh để vượt qua phần mềm bảo mật. Đó là ngụy trang nó như một Launcher cho một những trò chơi video phổ biến trên thế giới.
AZORult		Là một Trojan độc hại ăn cắp dữ liệu từ hệ thống bị nhiễm. - Phương thức lây lan: Các chiến dịch email spam thúc đẩy phần đính kèm độc hại (tài liệu MS Office) - Mục tiêu: đánh cắp thông tin ngân hàng, mật khẩu người dùng,… - Một số mốc thời gian đáng chú ý: Tháng 6/2018, AZORult được nâng cấp thành phiên bản 3.2,

		một phiên bản cạp nhật đáng kể, cải thiện thêm chức năng đánh cắp, lây lan và download. Tháng 2/2020, các chuyên gia trong lĩnh vực bảo mật đã phát hiện một chiến dịch mới của AZORult: lạm dụng dịch vụ ProtonVPN và thả phần mềm độc hại qua trình cài đặt ProtonVPN giả mạo cho Windows.