

Số: /BC-CATTT

Hà Nội, ngày tháng năm 2025

BÁO CÁO AN TOÀN THÔNG TIN MẠNG VIỆT NAM
(Tháng 12/2024)

Thực hiện chức năng quản lý nhà nước và tổ chức thực thi pháp luật về an toàn thông tin mạng, Cục An toàn thông tin phát hành Báo cáo An toàn thông tin định kỳ hàng tháng.

Báo cáo cung cấp thông tin về các sự kiện an toàn thông tin mạng, xu hướng tấn công mạng, các lỗ hổng an toàn thông tin mới được công bố... Thông tin này giúp các cơ quan, tổ chức nắm bắt kịp thời các vấn đề an toàn thông tin mạng đang diễn ra từ đó có thể chủ động triển khai kịp thời các biện pháp (con người, quy trình, công nghệ) để bảo đảm an toàn thông tin cho cơ quan, tổ chức mình.

Trong tháng **12/2024**, Cục An toàn thông tin (Bộ Thông tin và Truyền thông) đã phát hành các văn bản cảnh báo liên quan đến một số lỗ hổng mới đang tồn tại trong thực tế, cảnh báo về chiến dịch tấn công mã độc đến các cơ quan, tổ chức, doanh nghiệp.

Trong tháng **12/2024**, hệ thống giám sát, cảnh báo sớm rủi ro của Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC), Cục An toàn thông tin đã ghi nhận hàng trăm tên miền giả mạo các cơ quan, tổ chức tài chính, các ngân hàng nhằm mục tiêu lừa đảo người dân trên không gian mạng. Về nguy cơ, rủi ro mới, Trung tâm NCSC ghi nhận **12 lỗ hổng mới** có thể gây ra các nguy cơ **Nghiêm trọng** đến hệ thống thông tin. Trung tâm NCSC cũng đã phân tích và công bố danh sách các chỉ báo tấn công mạng (IoC) liên quan đến các chiến dịch tấn công có thể ảnh hưởng đến Việt Nam tại các đơn vị.

Đề nghị các đơn vị, tổ chức, doanh nghiệp nghiên cứu thông tin về các nguy cơ rủi ro trong báo cáo, thực hiện rà soát hệ thống, đánh giá **Tín nhiệm mạng** đối với hệ thống phục vụ giao dịch điện tử, xử lý các vấn đề về an toàn thông tin mạng và gửi kết quả báo cáo rà soát về địa chỉ thư điện tử **ncsc@ais.gov.vn chậm nhất trước ngày 25/01/2025**.

1. Cảnh báo an toàn thông tin đã phát hành trong tháng



Báo cáo về các lỗ hổng an toàn thông tin trong các sản phẩm của Microsoft tháng 12/2024.

Thông tin chi tiết tại:
<https://khonggianmang.vn/alert/lo-hong-bao-mat-co-muc-anh-huong-cao-va-nghiem-trong-trong-cac-san-pham-microsoft-cong-bo-thang-12-2024.260/>

Cảnh báo an toàn thông tin phát hành hàng tuần trên không gian mạng cung cấp thông tin kịp thời về các nguy cơ an toàn thông tin, lỗ hổng bảo mật và khuyến nghị kỹ thuật, giúp cơ quan và doanh nghiệp chủ động phòng ngừa và xử lý sự cố.

Thông tin chi tiết tại:
<https://khonggianmang.vn/>



2. Tình hình kết nối, chia sẻ dữ liệu giám sát

Tình hình kết nối, chia sẻ dữ liệu giám sát theo yêu cầu Chỉ thị số 14/CT-TTG năm 2019. Đến tháng **12/2024** 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). 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 **75/87** đơn vị có kết nối chia sẻ dữ liệu tương đối đầy đủ, **12/87** đơn vị không nhận được dữ liệu chia sẻ.

Theo ghi nhận từ Hệ thống kỹ thuật của Trung tâm Giám sát an toàn không gian mạng quốc gia cho thấy còn tồn tại nhiều đơn vị Bộ/Ngành, địa phương chưa thực hiện chia sẻ dữ liệu. Để đảm bảo an toàn hệ thống thông tin quốc gia, Cục An toàn thông tin đề nghị các đơn vị khẩn trương triển khai nghiêm túc và chặt chẽ các quy định theo chỉ thị của Thủ tướng Chính phủ để thực hiện việc chia sẻ dữ liệu nhằm đảm bảo tính liên thông, an toàn và hiệu quả trong quản lý và điều hành hệ thống thông tin quốc gia.

Ghi chú: Danh sách tình trạng triển khai công tác giám sát của các đơn vị tại **Phụ lục V** kèm theo.

Tình hình triển khai giải pháp phòng chống mã độc đáp ứng yêu cầu của Chỉ thị số 14/CT-TTG năm 2018. Đến tháng **12/2024** 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). Hiện nay, còn tồn tại 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.

Thông qua việc 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 **76/88 đơn vị** có kết nối thường xuyên. Trong các đơn vị kết nối thường xuyên có **76/76 đơn vị** chia sẻ về hệ điều hành các máy (**tổng số máy là 268.625**).

Ghi chú: Danh sách tình trạng triển khai giải pháp phòng chống mã độc của các đơn vị tại **Phụ lục VI** kèm theo.

3. Phát hiện và ngăn chặn, giảm thiểu lừa đảo trên không gian mạng

Thực hiện công tác kiểm tra, rà soát an toàn thông tin trên không gian mạng, Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC) đã ghi nhận **125.568 địa chỉ website** giả mạo cơ quan, tổ chức. Các đối tượng sử dụng website giả mạo này để lừa đảo, gây thiệt hại cho người dân trên không gian mạng, đồng

thời gây thiệt hại nghiêm trọng đến uy tín, thương hiệu của chính cơ quan, tổ chức bị giả mạo.

Mục tiêu hướng đến của các đối tượng lừa đảo là lừa đảo người dân thông qua giả mạo các website của cơ quan chức năng, các tổ chức tài chính – ngân hàng, các sàn thương mại điện tử, các công ty lớn...

Cục An toàn thông tin đã tích cực triển khai việc cấp chứng nhận Tín nhiệm mạng cho các hệ thống phục vụ giao dịch điện tử theo Nghị định 137/2024/NĐ-CP, tổng số hệ thống được cấp chứng nhận hiện đạt **6.038 hệ thống**.

Ghi chú: Các cơ quan, đơn vị có thể tra cứu thông tin, đăng ký Tín nhiệm mạng tại: <https://tinnhiemmang.vn/>.

Trong tháng **12/2024**, hệ thống của NCSC đã phát hiện **76 website** giả mạo thương hiệu với mục đích lừa đảo được phát tán trên không gian mạng. Đề nghị các đơn vị, tổ chức, doanh nghiệp cần chủ động rà quét, phát hiện sớm các website lừa đảo giả mạo tổ chức của mình, cảnh báo sớm đến người dùng của mình nhằm ngăn chặn các hoạt động lừa đảo đến người dùng, đảm bảo an toàn thông tin cho người dùng, bảo vệ chính thương hiệu của tổ chức.



Danh sách các website lừa đảo được cập nhật tại <https://alert.khonggianmang.vn/>

Ghi chú: Danh sách các website giả mạo đã phát hiện tại **Phụ lục I** kèm theo.

4. Phát hiện và cảnh báo sớm các lỗ hổng của các hệ thống thông tin trên không gian mạng

Thực hiện nhiệm vụ thu thập thông tin, tổng hợp, phân tích, theo dõi và dự báo, cảnh báo sớm xu hướng về các hoạt động, diễn biến trên không gian mạng Việt Nam. Trong tháng, Hệ thống giám sát kỹ thuật của NCSC đã ghi nhận có **784.180** điểm yếu, lỗ hổng an toàn thông tin tại các máy chủ, máy trạm, hệ thống thông tin của các cơ quan tổ chức nhà nước.

Ghi chú: Danh sách TOP 10 điểm yếu, lỗ hổng tồn tại phổ biến trên các máy của cơ quan, tổ chức tại **Phụ lục II** kèm theo.

Trong tháng **12/2024**, hệ thống giám sát, rà quét từ xa của Trung tâm NCSC đã phát hiện hơn **1600** lỗ hổng trên **5000** hệ thống đang mở công khai trên Internet.

Trung tâm NCSC cũng đã ghi nhận **12 lỗ hổng mới** được công bố, có mức độ ảnh hưởng **Nghiêm trọng/Cao** có thể bị lợi dụng để tấn công, khai thác vào các hệ thống của các cơ quan, tổ chức. Các lỗ hổng này là các lỗ hổng tồn tại trên các sản phẩm phổ biến của nhiều cơ quan, tổ chức, doanh nghiệp. Đề nghị các đơn vị cần thực hiện kiểm tra toàn diện và rà soát hệ thống của mình giúp xác định hệ thống của mình có sử dụng các sản phẩm bị ảnh hưởng bởi các lỗ hổng không, nhanh chóng đưa ra biện pháp khắc phục kịp thời để bảo vệ an toàn thông tin. Đồng thời, liên tục cập nhật thông tin về các lỗ hổng mới, các xu hướng tấn công trên không gian mạng.



Danh sách các lỗ hổng mới được cập nhật tại <https://alert.khonggianmang.vn/>

Thông kê các lỗ hổng đáng chú ý được ghi nhận trong tháng 12/2024:

TT	Mã điểm yếu/lỗ hổng	Mô tả	Ghi chú
1	CVE-2024-3393	<ul style="list-style-type: none"> - Điểm CVSS: Chưa xác định - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ - Ảnh hưởng: Palo Alto Networks PAN-OS - Lỗ hổng chưa có mã khai thác và đang bị khai thác trong thực tế 	https://nvd.nist.gov/vuln/detail/CVE-2024-3393
2	CVE-2024-41713	<ul style="list-style-type: none"> - Điểm CVSS: 7.5 (Cao) - Mô tả: Lỗ hổng cho phép đối tượng tấn công truy cập và thực hiện các hành vi trái phép - Ảnh hưởng: Mitel MiCollab 	https://nvd.nist.gov/vuln/detail/CVE-2024-41713

		- Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế	
3	CVE-2024-12856	- Điểm CVSS: 7.2 (Cao) - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã từ xa - Ảnh hưởng: Router hãng Four-Faith mẫu F3x24 và F3x36 - Lỗ hổng chưa có mã khai thác và đang bị khai thác trong thực tế	https://nvd.nist.gov/vuln/detail/CVE-2024-12856
4	CVE-2018-0802	- Điểm CVSS: 7.8 (Cao) - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã từ xa - Ảnh hưởng: Microsoft Office 2007, 2010, 2016 - Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế	https://nvd.nist.gov/vuln/detail/CVE-2018-0802
5	CVE-2024-49138	- Điểm CVSS: 7.8 (Cao) - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực hiện tấn công leo thang đặc quyền - Ảnh hưởng: Microsoft Windows 10, Windows 11, Windows Server 2008, 2012, 2016, 2019, 2022, 2025 - Lỗ hổng chưa có mã khai thác và đang bị khai thác trong thực tế	https://nvd.nist.gov/vuln/detail/CVE-2024-49138
6	CVE-2024-50623	- Điểm CVSS: 9.8 (Nghiêm trọng) - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã từ xa - Ảnh hưởng: Cleo Harmony, VLTrader, LexiCom - Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế	https://nvd.nist.gov/vuln/detail/CVE-2024-50623
7	CVE-2024-52046	- Điểm CVSS: 10.0 (Nghiêm trọng) - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã từ xa - Ảnh hưởng: Apache MINA	https://nvd.nist.gov/vuln/detail/CVE-2024-52046

		- Lỗ hổng chưa có mã khai thác và chưa bị khai thác trong thực tế	
8	CVE-2024-53677	- Điểm CVSS: 9.5 (Nghiêm trọng) - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã từ xa - Ảnh hưởng: Apache Struts - Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế	https://nvd.nist.gov/vuln/detail/CVE-2024-53677
9	CVE-2024-56337	- Điểm CVSS: Chưa xác định - Mô tả: Lỗ hổng cho phép đối tượng tấn công truy cập và thực thi các hành vi trái phép - Ảnh hưởng: Apache Tomcat - Lỗ hổng chưa có mã khai thác và đang bị khai thác trong thực tế	https://nvd.nist.gov/vuln/detail/CVE-2024-56337
10	CVE-2023-48788	- Điểm CVSS: 9.8 (Nghiêm trọng) - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã từ xa - Ảnh hưởng: FortiClientEMS - Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế	https://nvd.nist.gov/vuln/detail/CVE-2023-48788
11	CVE-2024-35250	- Điểm CVSS: 7.8 (Cao) - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực hiện tấn công leo thang đặc quyền - Ảnh hưởng: Microsoft Windows 10, Windows 11, Windows Server 2008, 2012, 2016, 2019, 2022 - Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế	https://nvd.nist.gov/vuln/detail/CVE-2024-35250
12	CVE-2024-20767	- Điểm CVSS: 7.4 (Cao) - Mô tả: Lỗ hổng cho phép đối tượng tấn công truy cập và thực hiện các hành vi trái phép - Ảnh hưởng: ColdFusion - Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế	https://nvd.nist.gov/vuln/detail/CVE-2024-20767

5. Phân tích rủi ro và cảnh báo sớm các nguy cơ tấn công có chủ đích

Thực hiện phân tích, theo dõi và dự báo, cảnh báo sớm xu hướng về tấn công mạng, Cục An toàn thông tin (Bộ Thông tin và Truyền thông) phát hiện xu hướng tấn công mã hóa tống tiền (ransomware) tăng cao trong thời gian gần đây. Đã có một số hệ thống thông tin của cơ quan, tổ chức, doanh nghiệp tại Việt Nam bị sự cố tấn công, gây gián đoạn hoạt động và thiệt hại về vật chất, hình ảnh của các cơ quan, tổ chức, doanh nghiệp, cũng như hoạt động bảo đảm an toàn không gian mạng quốc gia.

Trung tâm NCSC đã tiến hành thu thập, phân tích và phát hiện nhiều chỉ báo (Indicators of compromise) về tấn công mạng có thể ảnh hưởng đến cơ quan, tổ chức, doanh nghiệp Việt Nam. Các đơn vị cần chủ động rà soát các máy chủ, máy trạm, rà soát toàn bộ các hệ thống giám sát theo các chỉ báo mà Trung tâm NCSC cung cấp trong báo cáo nhằm xử lý sớm các rủi ro trong hệ thống, liên tục cập nhật các chỉ báo về tấn công mạng, đặc biệt là các chỉ báo đã được chia sẻ từ hệ thống của Trung tâm NCSC.



IOC	NHÓM TẤN CÔNG APT
103[.]91[.]64[.]214	Nhóm APT "Earth Estries"
aplusmodgovua.workers[.]dev	Nhóm APT "UAC-0125"
aplusdesktop.workers[.]dev	Nhóm APT "UAC-0125"
desktopaplus.workers[.]dev	Nhóm APT "UAC-0125"
wvtmsouaa2gt6jmcuxj5hkrqds5ihecoqjt5dl7gfrueu3i5mkad[.]onion	Nhóm APT "UAC-0125"
armyplus.workers[.]dev	Nhóm APT "UAC-0125"
armyplus-desktop.workers[.]dev	Nhóm APT "UAC-0125"

Thông tin IOC được cung cấp tại <https://alert.khonggianmang.vn/>

Ghi chú: Danh sách các IOC có thể ảnh hưởng tới cơ quan, tổ chức doanh nghiệp Việt Nam ghi nhận tại **Phụ lục III** kèm theo.

6. Phát hiện và cảnh báo sớm các nguy cơ botnet trong hệ thống

Thực hiện việc phân tích và phát hiện sớm các nguy cơ từ bên trong hệ thống, đặc biệt là các nguy cơ máy chủ, máy trạm trong hệ thống nhiễm mã độc, trở thành botnet. Hệ thống giám sát của NCSC đã thực hiện thu thập chia sẻ thông tin về các mối đe dọa trên không gian mạng với các tổ chức quốc tế, giám sát liên tục các mạng lưới botnet.

Trong tháng **12/2024**, Trung tâm NCSC phát hiện **20 hệ thống** của các đơn vị có kết nối đến hạ tầng botnet. Trung tâm NCSC đã thực hiện chia sẻ các thông tin botnet này đến các đơn vị thông qua hệ thống phát hiện cảnh báo sớm botnet.

Phát hiện **100+** hệ thống bị lây nhiễm mã độc botnet trong tháng

TỔ CHỨC BỊ ẢNH HƯỞNG	ĐỊA CHỈ IP CÁC	CÔNG KẾT NỐI CÁC
[Mờ]	210.86.230.212	80
[Mờ]	117.6.130.78	80
[Mờ]	113.163.94.8	80
[Mờ]	113.163.202.128	80
[Mờ]	113.161.184.151	80
[Mờ]	113.160.165.121	80
[Mờ]	113.161.204.167	80

Xem thêm

Thông tin các hệ thống ghi nhận nhiễm botnet trên hệ thống phát hiện cảnh báo sớm.

Ghi chú: Danh sách các đơn vị có địa chỉ IP nằm trong botnet ghi nhận tại Phụ lục IV kèm theo.

Đề nghị các đơn vị, tổ chức, doanh nghiệp nghiên cứu các thông tin về các nguy cơ rủi ro trong báo cáo, thực hiện rà soát hệ thống, xử lý các vấn đề về an toàn thông tin mạng trong hệ thống. Trong quá trình thực hiện, nếu có thông tin cần hỗ trợ đề nghị liên hệ với Trung tâm Giám sát an toàn không gian mạng quốc gia, Cục An toàn thông tin, Bộ Thông tin và Truyền thông, điện thoại: 024.3209.1616 hoặc số điện thoại trực đường dây nóng hỗ trợ giám sát, cảnh báo sớm 0961.405.333, thư điện tử: ncsc@ais.gov.vn./.

Nơi nhận:

- Thứ trưởng Phạm Đức Long (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 Tập đoàn kinh tế và Tổng công ty nhà nước;
- Các Tổ chức tài chính, Ngân hàng thương mại nhà nước;
- Ngân hàng Thương mại Cổ phần;
- Ngân hàng Chính sách xã hội;
- Ngân hàng Phát triển Việt Nam;
- Ngân hàng Hợp tác xã Việt Nam;
- Các công ty Cổ phần Chứng khoán;
- Các Tổ chức, doanh nghiệp hoạt động trong lĩnh vực thương mại điện tử;
- Các tổ chức, doanh nghiệp cung cấp dịch vụ trung gian thanh toán, ví điện tử;
- Các Cục: Viễn thông, Bưu điện Trung ương;
- Các Trung tâm: TTTT, VNNIC;
- Các doanh nghiệp: VNPOST, VTC;
- Các phòng: ATHTTT, TT&HTQT;
- Trung tâm VNCERT/CC;
- Lưu: VT, NCSC.LTQ.

Q. CỤC TRƯỞNG

Trần Quang Hưng

Phụ lục I
DANH SÁCH CÁC WEBSITE GIẢ MẠO, LỪA ĐẢO PHÁT HIỆN
TRONG THÁNG

(Kèm theo Báo cáo số /BC-CATTT ngày tháng năm 2025
của Cục An toàn thông tin)

TT	Website giả mạo	Ghi chú
1	amazoui[.]top	Website giả mạo sàn TMĐT Amazon
2	http://amazoni1[.]com	Website giả mạo sàn TMĐT Amazon
3	www[.]amzzcbe-cme[.]com	Website giả mạo sàn TMĐT Amazon
4	https://sellings-global[.]com/shop	Website giả mạo sàn TMĐT Amazon
5	https://amazoni1[.]com/	Website giả mạo sàn TMĐT Amazon
6	https://amazouo9[.]com/	Website giả mạo sàn TMĐT Amazon
7	applecenter[.]info[.]vn	Website giả mạo Apple
8	https://www[.]digibox[.]info[.]vn/airpods3?utm_campaign=Long%20-%20digibox%20-%20nu%C3%B4i%2001&utm_content=02&fbclid=IwZXh0bgNhZW0BMABhZGlkAasZCGz5JSwBHT5sNmX5CobI-mFmyxkQnvPB-vmhPSuhE1LUhMIFckHiaDekcYOhFHgkMg_aem__29GzKkOofyqX5qAXDWtJg&utm_medium=paid&utm_source=fb&utm_id=120217338962780188&utm_term=120217338962790188&zarsrc=1303&gidzl=FgfK5z	Website giả mạo Apple

	7RkoW-jb8OryQ- 9ZIpkN70aUeW8hDH4i70ldOkkWS Naidc8YpfNHJ5pmmhU- y673NQGzW7rzcu8W	
9	https://dichvucong[.]xqrgov[.]com/	Website giả mạo Bộ Công An
10	https://dichvucong[.]hokhauso[.]com	Website giả mạo Bộ Công An
11	dichvucong[.]thongtincancuoc[.]org	Website giả mạo Bộ Công An
12	https://mofvn[.]com/	Website giả mạo Bộ Tài chính
13	vietchinhphu[.]com	Website giả mạo Cổng Dịch vụ công Quốc gia
14	https://giaohangtietkiem[.]com/	Website giả mạo Công ty cổ phần giao hàng tiết kiệm
15	https://chat[.]dichvutonghop[.]vip/mobile/index?code=5dNnwAlZmXa8ELYdy3FnUESBYQgLpcZ5jKi4MYA3XOG1NLxUpNmNLWcmz12qHQoQlj2s4iXw%2FzjgvtmomDR0VshLNZtBAxBLxRoBsOnRh8%2FS7vKKZuG9IF1RoudmuJT4X%2Fc	Website giả mạo Công ty cổ phần giao hàng tiết kiệm
16	dichvugiaohangtietkiemvn[.]store	Website giả mạo Công ty cổ phần giao hàng tiết kiệm
17	https://giaohangtietkiem[.]com[.]vn/	Website giả mạo Công ty cổ phần giao hàng tiết kiệm
18	https://dichvugiaohangtietkiemvn[.]pro/	Website giả mạo Công ty cổ phần giao hàng tiết kiệm
19	aeonmaills[.]shop	Website giả mạo Công ty TNHH Aeon Việt Nam
20	https://aeonmaills[.]shop	Website giả mạo Công ty TNHH Aeon Việt Nam

21	https://www[.]cuisin[.]sa[.]com/	Website giả mạo Cục An toàn thông tin, Bộ Thông tin và Truyền thông
22	https://cucanninhmang24h[.]com/?gad_source=1&gclid=CjwKCAiAyJS7BhBiEiwAyS9uNc-iPjBdOOzmxG_eHcDcmdg_Ekr23sT1FbmDx9b70p4qSck4Y-8jRhoCX6gQAvD_BwE	Website giả mạo Cục An toàn thông tin, Bộ Thông tin và Truyền thông
23	https://dienmayxanh-services[.]com/	Website giả mạo Điện máy xanh
24	https://magiamgiadienmayxanh[.]com/dmx/	Website giả mạo Điện máy xanh
25	https://dienmay-xanh24h[.]online/?gad_source=1&gclid=CjwKCAiAgoq7BhBxEiwAVcW0LF-Eji5e6PR_CcQ0EVVuMz__QF4Jk8W6UdtvL1gDsMUkd2g1nG41HBoCR9MQAvD_BwE	Website giả mạo Điện máy xanh
26	https://www[.]ebayglobal[.]shop/home	Website giả mạo sàn TMĐT Ebay
27	https://mfacebook-com[.]vn/JdS5I1scWRo8PdQOeyKQdW	Website giả mạo Facebook
28	https://mfacebook-com[.]vn	Website giả mạo Facebook
29	https://giaohangnhanh88[.]com/	Website giả mạo Giao hàng nhanh
30	https://da6555[.]com/order/play	Website giả mạo sàn TMĐT Lazada
31	https://thuongmdientu[.]shop/index/index/home[.]html	Website giả mạo sàn TMĐT Lazada
32	https://da5651[.]com	Website giả mạo sàn TMĐT Lazada

33	http://www[.]lazadass[.]com/#/	Website giả mạo sàn TMĐT Lazada
34	my-renewal-log[.]com	Website giả mạo Netflix
35	xjp[.]morganfutureszy[.]com	Website giả mạo Ngân hàng JP Morgan Chase Bank Mỹ tại Việt Nam
36	https://cskh-techcombank[.]com/	Website giả mạo Ngân hàng TMCP Kỹ Thương Việt Nam
37	cskh-techcombank[.]com	Website giả mạo Ngân hàng TMCP Kỹ Thương Việt Nam
38	hdbank[.]khuyenmaikhachhang-triankhachhang-thang12[.]com[.]vn	Website giả mạo Ngân hàng TMCP Phát triển Thành phố Hồ Chí Minh
39	https://mbtaichinh-tienloi[.]com/	Website giả mạo Ngân hàng TMCP Quân đội
40	https://tc-shbfinance[.]com/	Website giả mạo Ngân hàng TMCP Sài Gòn – Hà Nội
41	mail[.]vpbank[.]chamsockhachhang-khuyenmaithe-hotro247-thang12[.]com[.]vn	Website giả mạo Ngân hàng TMCP Việt Nam Thịnh Vượng
42	vpbank[.]uudaithe-chamsockhachhang-capnhatthe-thang12[.]com[.]vn	Website giả mạo Ngân hàng TMCP Việt Nam Thịnh Vượng
43	vpbank[.]hotrotructuyen-chamsockhachhang-hotro247-thang12[.]com[.]vn	Website giả mạo Ngân hàng TMCP Việt Nam Thịnh Vượng
44	mail[.]vpbank[.]hotrotructuyen-chamsockhachhang-hotro247-thang12[.]com[.]vn	Website giả mạo Ngân hàng TMCP Việt Nam Thịnh Vượng
45	https://shinhan[.]hotrokhachhang-hotrotructuyen-uudaidacbiet-thang12[.]com[.]vn/	Website giả mạo Ngân hàng TNHH MTV Shinhan Việt Nam
46	https://shinhan[.]chamsocthe-uudai-khachhang-tructuyen[.]com[.]vn/	Website giả mạo Ngân hàng TNHH MTV Shinhan Việt Nam

47	https://shinhan[.]hotrotructuyen-khachhangcanhanthang12[.]com[.]vn /	Website giả mạo Ngân hàng TNHH MTV Shinhan Việt Nam
48	www[.]sp66699[.]com	Website giả mạo sàn TMĐT Shopee
49	https://sp6708p[.]com	Website giả mạo sàn TMĐT Shopee
50	https://sp5583p[.]com	Website giả mạo sàn TMĐT Shopee
51	https://nzu23516s[.]com/	Website giả mạo sàn TMĐT Shopee
52	https://kph25332s[.]com/	Website giả mạo sàn TMĐT Shopee
53	https://www[.]starbucks.vn/lucky-bag?utm_source=Starbucks&utm_campaign=DD&fbclid=IwZXh0bgNhZW0BMABhZG1kAasV5gBd-3wBHdRd8ptz_TEEdgrMhr0N0mVFIVI_uBkfSE2GQY923iqQ5ezsmRlQuI-IWw_aem_Ec4U1tVW2HMhiIR8TX_eaQ	Website giả mạo Starbucks
54	https://www[.]tbaovn-cms[.]top	Website giả mạo sàn TMĐT Taobao
55	https://www[.]tbaovn-cms[.]top/shops/create?invitation_code=8573	Website giả mạo sàn TMĐT Taobao
56	https://tbaovn-cms[.]top/	Website giả mạo sàn TMĐT Taobao
57	https://marketing-oder[.]com/login	Website giả mạo sàn TMĐT Taobao
58	https://affiliatetaobao[.]org/	Website giả mạo sàn TMĐT Taobao

59	evn[.]brvgov[.]com	Website giả mạo Tập đoàn Điện lực Việt Nam (EVN)
60	https://landing[.]levnpoint[.]com/	Website giả mạo Tập đoàn Điện lực Việt Nam (EVN)
61	https://pvldumsvop[.]xin/	Website giả mạo Telegram
62	https://suatuoihanam-thtruemilk[.]com	Website giả mạo TH true MILK
63	https://tikiethongmuasam12h[.]com/my	Website giả mạo sàn TMĐT Tiki
64	ozonvietnam[.]com	Website giả mạo sàn TMĐT Tiki
65	https://tiktok[.]jegabw[.]com	Website giả mạo TikTok
66	https://nappxutiktok[.]com	Website giả mạo TikTok
67	https://tiktok-svip61[.]com/r?code=SRDONN	Website giả mạo TikTok
68	https://evaluatetravels[.]com/login	Website giả mạo Traveloka
69	chinhphu[.]kbshkdt[.]org	Website giả mạo Văn phòng Chính phủ
70	chinhphu[.]khaibaoshkdt[.]com	Website giả mạo Văn phòng Chính phủ
71	chinhphuvn[.]cc	Website giả mạo Văn phòng Chính phủ
72	Vtp-vandon[.]online	Website giả mạo ViettelPost
73	viettelpost-vn[.]jicu	Website giả mạo ViettelPost
74	https://vincomplaza[.]y7f[.]top/	Website giả mạo Vincom
75	corona[.]vinpearl668[.]com/	Website giả mạo Vinpearl

76	quocte[.]click	Website giả mạo Western Union
----	----------------	-------------------------------

Phụ lục II
MỘT SỐ LỖ HỔNG VẪN CÒN TỒN TẠI PHỔ BIẾN TRÊN CÁC MÁY
CỦA CƠ QUAN TỔ CHỨC

*(Kèm theo Báo cáo số /BC-CATTT ngày tháng năm 2025
của Cục An toàn thông tin)*

TT	Mã điểm yếu/ lỗ hổng	SL máy bị ảnh hưởng	Ghi chú
1	CVE-2024-49138	7292	https://nvd.nist.gov/vuln/detail/ CVE-2022-49138
2	CVE-2022-26809	6267	https://nvd.nist.gov/vuln/detail/ CVE-2022-26809
3	CVE-2023-21716	2845	https://nvd.nist.gov/vuln/detail/ CVE-2023-21716
4	CVE-2024-49046	2830	https://nvd.nist.gov/vuln/detail/ CVE-2024-49046
5	CVE-2024-49576	2775	https://nvd.nist.gov/vuln/detail/ CVE-2024-49576
6	CVE-2023-40477	2468	https://nvd.nist.gov/vuln/detail/ CVE-2023-40477
7	CVE-2023-38831	2123	https://nvd.nist.gov/vuln/detail/ CVE-2023-38831
8	CVE-2024-38261	2077	https://nvd.nist.gov/vuln/detail/ CVE-2024-38261
9	CVE-2024-49083	2065	https://nvd.nist.gov/vuln/detail/ CVE-2024-49083
10	CVE-2024-6197	1831	https://nvd.nist.gov/vuln/detail/ CVE-2024-6197

Phụ lục III
THỐNG KÊ CÁC THÔNG TIN CHỈ BÁO (INDICATORS OF
COMPROMISE)

*(Kèm theo Báo cáo số /BC-CATTT ngày tháng năm 2024
của Cục An toàn thông tin)*

STT	Indicators of compromise	Ghi chú
1	103[.]91[.]64[.]214	Nhóm APT “Earth Estries”
2	23[.]81[.]41[.]166	
3	172[.]93[.]165[.]14	
4	103[.]75[.]190[.]73	
5	43[.]226[.]126[.]164	
6	193[.]239[.]86[.]168	
7	146[.]70[.]79[.]105	
8	165[.]154[.]227[.]192	
9	158[.]247[.]222[.]165	
10	91[.]245[.]253[.]27	
11	45[.]125[.]67[.]144	
12	172[.]93[.]165[.]10	
13	146[.]70[.]79[.]18	
14	205[.]189[.]160[.]3	
15	pulseathermakf[.]com	
16	www[.]infraredsen[.]com	

17	billing[.]clothworls[.]com		
18	helpdesk[.]stnekpro[.]com		
19	jasmine[.]lhousewares[.]com		
20	private[.]royalnas[.]com		
21	vpn487875652[.]softether[.]net		
22	96[.]9[.]211[.]27		
23	139[.]59[.]108[.]43		
24	143[.]198[.]92[.]175		
25	139[.]59[.]236[.]31		
26	vpn114240349[.]softether[.]net		
27	imap[.]dateupdata[.]com		
28	139[.]99[.]114[.]108		
29	cookiemanager.n-e[.]kr		Nhóm APT “Kimsuky”
30	naverbox.p-e[.]kr		
31	ned.kesug[.]com		
32	owna.loveslife[.]biz		
33	185.27.134[.]201		
34	185.27.134[.]140		
35	185.27.134[.]120		

36	nidiogln.n-e[.]kr	
37	covd.2kool4u[.]net	
38	wud.wuaze[.]com	
39	evangelia[.]edu	
40	185.105.33[.]106	
41	185.27.134[.]93	
42	185.27.134[.]144	
43	38.60.146[.]78:443	Chiến dịch tấn công triển khai mã độc PlugX
44	45.123.188[.]180	
45	118.107.219[.]66:443	
46	198.244.237[.]131	
47	desktopapluscom.workers[.]dev	Nhóm APT “UAC-0125”
48	armyplus-desktop.workers[.]dev	
49	armylpus.workers[.]dev	
50	wvtmsouaa2gt6jmcuxj5hkfrqdss5lh ecoqijt5dl7gfruueu3i5mkad[.]onion	
51	desktopaplus.workers[.]dev	
52	aplustesktop.workers[.]dev	
53	aplustmodgovua.workers[.]dev	

Phụ lục IV
DANH SÁCH CÁC ĐƠN VỊ CÓ ĐỊA CHỈ IP NẴM TRONG MẠNG
BOTNET

(Kèm theo Báo cáo số /BC-CATTT ngày tháng năm 2025
của Cục An toàn thông tin)

1. Danh sách Bộ/Ngành

TT	Tên đơn vị	Số lượng IP botnet tháng 11/2024	Số lượng IP botnet tháng 12/2024	Loại mã độc/botnet
1	Bộ Khoa học và Công nghệ	3	1	Andromeda
2	Đài tiếng nói Việt Nam	0	1	Andromeda

2. Danh sách Tỉnh/thành

STT	Tên đơn vị	Số lượng IP botnet tháng 11/2024	Số lượng IP botnet tháng 12/2024	Ghi chú
1	Lai Châu	3	6	Andromeda
2	Nam Định	4	6	Andromeda
3	Lâm Đồng	3	3	Andromeda
4	Điện Biên	1	2	Andromeda
5	Hà Nam	2	2	Andromeda
6	Hà Nội	1	2	Andromeda
7	Thái Bình	2	2	Andromeda
8	An Giang	0	1	Andromeda
9	Bến Tre	0	1	Andromeda
10	Cần Thơ	1	1	Andromeda

11	Cao Bằng	1	1	Andromeda
12	Hà Giang	0	1	Andromeda
13	Lạng Sơn	1	1	Andromeda
14	Lào Cai	1	1	Andromeda
15	Ninh Bình	1	1	Andromeda
16	Quảng Ninh	1	1	Andromeda
17	Thanh Hóa	2	1	Andromeda
18	Trà Vinh	0	1	Andromeda

Phụ lục V
TÌNH HÌNH KẾT NỐI, CHIA SẺ DỮ LIỆU GIÁM SÁT
THEO YÊU CẦU CHỈ THỊ SỐ 14/CT-TTG NĂM 2019

(Kèm theo Báo cáo số /BC-CATTT ngày tháng năm 2025
của Cục An toàn thông tin)

1. Danh sách Bộ/Ngành

TT	Bộ/Ngành/Cơ quan trực thuộc Chính phủ	Thời gian bắt đầu chia sẻ dữ liệu	Thời gian gần nhất nhận được dữ liệu (tính đến 31/12/2024)
1	Bộ Công Thương	09/08/2020	31/12/2024
2	Bộ Giáo dục và Đào tạo	31/08/2020	Không nhận được dữ liệu chia sẻ
3	Bộ Giao thông vận tải	15/05/2020	Không nhận được dữ liệu chia sẻ
4	Bộ Kế hoạch và Đầu tư	20/11/2020	Không nhận được dữ liệu chia sẻ
5	Bộ Khoa học và Công nghệ	19/11/2020	31/12/2024
6	Bộ Lao động - Thương Binh và Xã hội	11/12/2020	Không nhận được dữ liệu chia sẻ
7	Bộ Ngoại giao	24/07/2020	31/12/2024
8	Bộ Nội vụ	30/07/2020	31/12/2024
9	Bộ Nông nghiệp và Phát triển nông thôn	28/09/2020	Không nhận được dữ liệu chia sẻ
10	Bộ Tài chính	15/12/2020	31/12/2024
11	Bộ Tài nguyên và Môi trường	03/10/2020	31/12/2024
12	Bộ Thông tin và Truyền thông	11/02/2022	31/12/2024
13	Bộ Tư pháp	18/03/2023	31/12/2024
14	Bộ Văn hóa, Thể thao và Du lịch	20/06/2020	31/12/2024
15	Bộ Xây Dựng	23/07/2020	Không nhận được dữ liệu chia sẻ
16	Bộ Y tế	17/07/2020	Không nhận được dữ liệu chia sẻ

17	Ngân hàng Nhà nước Việt Nam	02/07/2020	31/12/2024
18	Thanh tra Chính phủ	10/11/2020	31/12/2024
19	Ủy ban Dân tộc	08/10/2020	31/12/2024
20	Văn phòng Chính phủ	22/09/2020	Không nhận được dữ liệu chia sẻ
21	Bảo Hiểm Xã Hội	08/11/2020	31/12/2024
22	Đài Truyền hình Việt Nam	14/09/2020	31/12/2024
23	Viện Hàn Lâm KHCN	22/09/2020	Không nhận được dữ liệu chia sẻ
24	Kiểm toán Nhà nước Việt Nam	09/03/2021	31/12/2024

2. Danh sách Tỉnh/Thành

TT	Tỉnh/Thành	Thời gian bắt đầu chia sẻ dữ liệu	Thời gian gần nhất nhận được dữ liệu (tính đến 31/12/2024)
1	An Giang	30/09/2020	30/12/2024
2	Bắc Giang	21/08/2020	31/12/2024
3	Bắc Kạn	01/09/2020	31/12/2024
4	Bạc Liêu	09/10/2020	Không nhận được dữ liệu chia sẻ
5	Bắc Ninh	23/07/2020	31/12/2024
6	Bà Rịa - Vũng Tàu	20/07/2020	31/12/2024
7	Bến Tre	10/08/2020	31/12/2024
8	Bình Định	05/06/2020	31/12/2024
9	Bình Dương	24/04/2020	31/12/2024
10	Bình Phước	23/04/2020	31/12/2024
11	Bình Thuận	31/08/2020	31/12/2024
12	Cà Mau	15/05/2020	31/12/2024
13	Cần Thơ	13/04/2020	31/12/2024
14	Cao Bằng	14/08/2020	31/12/2024
15	Đắk Lắk	17/06/2020	31/12/2024
16	Đắk Nông	31/08/2020	31/12/2024
17	Đà Nẵng	09/06/2020	20/12/2024
18	Điện Biên	02/06/2020	31/12/2024
19	Đồng Nai	15/06/2020	31/12/2024
20	Đồng Tháp	14/07/2020	31/12/2024
21	Gia Lai	14/09/2020	30/12/2024
22	Hà Giang	18/08/2020	12/12/2024
23	Hải Dương	04/09/2020	Không nhận được dữ liệu chia sẻ
24	Hải Phòng	28/07/2020	31/12/2024
25	Hà Nam	22/09/2020	31/12/2024
26	Hà Nội	30/06/2020	31/12/2024

27	Hà Tĩnh	06/10/2020	31/12/2024
28	Hòa Bình	13/05/2020	30/12/2024
29	Hồ Chí Minh	26/06/2020	31/12/2024
30	Hậu Giang	02/10/2020	31/12/2024
31	Hưng Yên	22/05/2020	31/12/2024
32	Khánh Hòa	21/09/2020	19/12/2024
33	Kiên Giang	24/09/2020	31/12/2024
34	Kon Tum	28/09/2020	31/12/2024
35	Lai Châu	26/09/2020	30/12/2024
36	Lâm Đồng	22/10/2020	27/12/2024
37	Lạng Sơn	08/10/2020	31/12/2024
38	Lào Cai	09/07/2020	31/12/2024
39	Long An	22/07/2020	9/12/2024
40	Nam Định	21/09/2020	31/12/2024
41	Nghệ An	09/09/2020	31/12/2024
42	Ninh Bình	28/07/2020	31/12/2024
43	Ninh Thuận	01/09/2020	31/12/2024
44	Phú Thọ	01/10/2020	31/12/2024
45	Phú Yên	30/11/2020	31/12/2024
46	Quảng Bình	01/07/2020	31/12/2024
47	Quảng Nam	14/09/2020	Không nhận được dữ liệu chia sẻ
48	Quảng Ngãi	12/08/2020	31/12/2024
49	Quảng Ninh	12/09/2020	31/12/2024
50	Quảng Trị	24/12/2020	31/12/2024
51	Sóc Trăng	12/08/2020	24/12/2024
52	Sơn La	13/07/2020	31/12/2024
53	Tây Ninh	08/07/2020	31/12/2024
54	Thái Bình	25/06/2020	31/12/2024
55	Thái Nguyên	19/11/2020	31/12/2024
56	Thanh Hóa	29/09/2020	31/12/2024

57	Thừa Thiên Huế	29/07/2020	31/12/2024
58	Tiền Giang	24/09/2020	31/12/2024
59	Trà Vinh	29/07/2020	31/12/2024
60	Tuyên Quang	19/11/2020	31/12/2024
61	Vĩnh Long	25/06/2020	31/12/2024
62	Vĩnh Phúc	30/06/2020	31/12/2024
63	Yên Bái	26/08/2020	27/12/2024

Phụ lục VI
TÌNH HÌNH TRIỂN KHAI GIẢI PHÁP PHÒNG CHỐNG MÃ ĐỘC ĐÁP
ỨNG YÊU CẦU CỦA CHỈ THỊ SỐ 14/CT-TTG NĂM 2018

(Kèm theo Báo cáo số /BC-CATTT ngày tháng năm 2025
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 máy chia sẻ dữ liệu trong tháng 12/2024	Ghi chú
1	Bộ Công Thương	204	
2	Bộ Giáo dục và Đào tạo	0	Chưa chia sẻ
3	Bộ Giao thông vận tải	91	
4	Bộ Kế hoạch và Đầu tư	19422	
5	Bộ Khoa học và Công nghệ	448	
6	Bộ Lao động - Thương Binh và Xã hội	0	Mất kết nối 01 tháng trở lên
7	Bộ Ngoại giao	11	
8	Bộ Nội vụ	417	
9	Bộ Nông nghiệp và Phát triển nông thôn	0	Chưa chia sẻ
10	Bộ Tài chính	270	
11	Bộ Tài nguyên và Môi trường	2010	
12	Bộ Thông tin và Truyền thông	294	
13	Bộ Tư pháp	0	Mất kết nối 01 tháng trở lên
14	Bộ Văn hóa, Thể thao và Du lịch	0	Mất kết nối 01 tháng trở lên
15	Bộ Xây Dựng	30	
16	Bộ Y tế	70	

17	Ngân hàng Nhà nước Việt Nam	2992	
18	Thanh tra Chính phủ	0	Mất kết nối 01 tháng trở lên
19	Ủy ban Dân tộc	0	Chưa chia sẻ
20	Văn phòng Chính phủ	0	Mất kết nối 01 tháng trở lên
21	Ban Quản lý Lăng Chủ tịch Hồ Chí Minh	0	Mất kết nối 01 tháng trở lên
22	Bảo Hiểm Xã Hội	20025	
23	Đài tiếng nói Việt Nam	10	
24	Đài Truyền hình Việt Nam	180	
25	Thông tấn xã Việt Nam	1683	
26	Viện Hàn Lâm KHCN	109	
27	Viện Hàn Lâm KHXH	0	Mất kết nối 01 tháng trở lên
28	Kiểm toán Nhà nước Việt Nam	0	Mất kết nối 01 tháng trở lên

2. Danh sách Tỉnh/Thành

TT	Tỉnh/Thành	Số lượng máy chia sẻ dữ liệu trong tháng 12/2024	Ghi chú
1	An Giang	442	
2	Bắc Giang	6188	
3	Bắc Kạn	2650	
4	Bạc Liêu	1893	
5	Bắc Ninh	1598	
6	Bà Rịa - Vũng Tàu	23545	
7	Bến Tre	1615	
8	Bình Định	166	
9	Bình Dương	1896	
10	Bình Phước	4686	
11	Bình Thuận	3788	
12	Cà Mau	1787	
13	Cần Thơ	0	Mất kết nối 01 tháng trở lên
14	Cao Bằng	1329	
15	Đắk Lắk	5205	
16	Đắk Nông	1098	

17	Đà Nẵng	40400	
18	Điện Biên	3523	
19	Đồng Nai	0	Mất kết nối 01 tháng trở lên
20	Đồng Tháp	4303	
21	Gia Lai	19	
22	Hà Giang	9	
23	Hải Dương	1821	
24	Hải Phòng	4280	
25	Hà Nam	937	
26	Hà Nội	17640	
27	Hà Tĩnh	2915	
28	Hòa Bình	1192	
29	Hồ Chí Minh	11410	
30	Hậu Giang	1212	
31	Hưng Yên	463	
32	Khánh Hòa	2209	
33	Kiên Giang	2174	
34	Kon Tum	5232	

35	Lai Châu	33	
36	Lâm Đồng	1903	
37	Lạng Sơn	276	
38	Lào Cai	2	
39	Long An	2934	
40	Nam Định	40	
41	Nghệ An	4819	
42	Ninh Bình	634	
43	Ninh Thuận	659	
44	Phú Thọ	0	Mất kết nối 01 tháng trở lên
45	Phú Yên	164	
46	Quảng Bình	2322	
47	Quảng Nam	245	
48	Quảng Ngãi	4142	
49	Quảng Ninh	0	Mất kết nối 01 tháng trở lên
50	Quảng Trị	321	
51	Sóc Trăng	29	
52	Son La	3707	

53	Tây Ninh	1043	
54	Thái Bình	3048	
55	Thái Nguyên	1968	
56	Thanh Hóa	1344	
57	Thừa Thiên Huế	6266	
58	Tiền Giang	7337	
59	Trà Vinh	1361	
60	Tuyên Quang	3347	
61	Vĩnh Long	3407	
62	Vĩnh Phúc	10523	
63	Yên Bái	860	

Ghi chú:

- Số lượng máy của mỗi đơn vị được tính dựa trên số lượng máy chia sẻ thông tin về hệ điều hành (trường “OS” trong 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 phát hành).