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 16 tháng 07năm 2024

BÁO CÁO AN TOÀN THÔNG TIN MẠNG VIỆT NAM
(Tháng 6/2024)

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 **6/2024**, 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 **6/2024**, 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 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 và gửi kết quả báo cáo rà soát về địa chỉ thư điện tử **ncsc@ais.gov.vn chậm nhất trước ngày 25/7/2024.**

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

Văn bản số 1096/CATTT-NCSC về việc lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 06/2024 phát hành ngày 14/06/2024.

Văn bản số 1095/CATTT-NCSC về việc cảnh báo nhóm APT "Mustang Panda" thực hiện chiến dịch tấn công nhằm vào Việt Nam phát hành ngày 14/06/2024.

Văn bản số 2516/BTTTT-CATTT; văn bản số 2517/BTTT-CATTT; văn bản số 2518/BTTTT-CATTT gửi các bộ ngành, địa phương, cơ quan, doanh nghiệp về việc hướng dẫn giải pháp tăng cường bảo đảm an toàn hệ thống thông tin phát hành ngày 27/06/2024.

2. Tình hình kết nối, chia sẻ dữ liệu của các bộ ngành địa phương

Tình hình kết nối, chia sẻ dữ liệu giám sát theo yêu cầu Chỉ thị số 14/CT-TTG năm 2019. Đến tháng **6/2024** 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 **71/87** đơn vị có kết nối chia sẻ dữ liệu tương đối đầy đủ, **16/87** 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, theo chỉ đạo của Cục trưởng 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.*

Tính hình triển khai giải pháp phòng chống mã độc đáp ứng yêu cầu của Chỉ thị số 14/CT-TTG năm 2018. Đến tháng **6/2024** 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 **83/88 đơn vị** có kết nối thường xuyên. Trong các đơn vị kết nối thường xuyên có **83/83 đơn vị** chia sẻ về hệ điều hành các máy **(tổng số máy là 275.169)**.

Ghi chú: *Danh sách trình 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 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 **124.928 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...

Trong tháng **6/2024**, hệ thống của NCSC đã phát hiện **68 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 **90.033** 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 **6/2024**, 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/

Thống kê các lỗ hổng đáng chú ý được ghi nhận trong tháng 6/2024:

TT	Mã điểm yếu/lỗ hổng	Mô tả	Ghi chú
1	CVE-2024-4577	- Điểm CVSS: 9.8 (Nghiêm trọng) - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã tùy ý, truy cập và thực hiện các hành vi trái phép. - Ảnh hưởng: Ngôn ngữ lập trình PHP.	https://nvd.nist.gov/vuln/detail/CVE-2024-4577

		- Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.	
2	CVE-2024-24919	- Điểm CVSS: 8.6 (Cao) - Mô tả: Lỗ hổng cho phép đối tượng tấn công truy cập và thực hiện các hành vi trái phép. - Ảnh hưởng: Check Point Security Gateways. - Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.	https://nvd.nist.gov/vuln/detail/CVE-2024-24919
3	CVE-2024-28995	- 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: SolarWinds Serv-U. - Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.	https://nvd.nist.gov/vuln/detail/CVE-2024-28995
4	CVE-2024-4358	- Điểm CVSS: 9.8 (Nghiêm trọng) - Mô tả: Lỗ hổng cho phép đối tượng tấn công truy cập và thực hiện các hành vi trái phép. - Ảnh hưởng: Progress Telerik Report Server. - Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.	https://nvd.nist.gov/vuln/detail/CVE-2024-4358
5	CVE-2017-3506	- 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: Oracle WebLogic Server. - Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.	https://nvd.nist.gov/vuln/detail/CVE-2017-3506

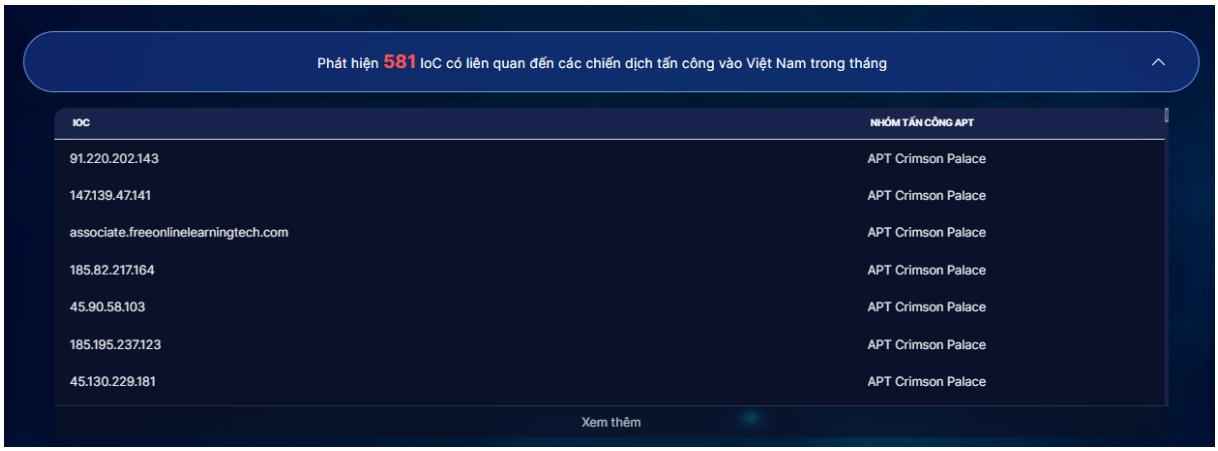
6	CVE-2024-37079	- Điểm CVSS: 9.8 (Nghiêm trọng) - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã từ xa, truy cập và thực hiện các hành vi trái phép. - Ảnh hưởng: VMware vCenter Server. - Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.	https://nvd.nist.gov/vuln/detail/CVE-2024-37079
7	CVE-2024-37080	- Điểm CVSS: 9.8 (Nghiêm trọng) - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã từ xa, truy cập và thực hiện các hành vi trái phép. - Ảnh hưởng: VMware vCenter Server. - Lỗ hổng đang bị khai thác trong thực tế.	https://nvd.nist.gov/vuln/detail/CVE-2024-37080
8	CVE-2024-26169	- Điểm CVSS: 7.8 (Cao) - Mô tả: Lỗ hổng cho phép đối tượng tấn công leo thang đặc quyền trên hệ thống. - Ảnh hưởng: Microsoft Windows 10. - Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.	https://nvd.nist.gov/vuln/detail/CVE-2024-26169
9	CVE-2024-5276	- Điểm CVSS: 9.8 (Nghiêm trọng) - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực hiện SQL Injection, qua đó truy cập và thực hiện các hành vi trái phép. - Ảnh hưởng: Fortra FileCatalyst Workflow. - Lỗ hổng chưa có mã khai thác hay bị khai thác trong thực tế.	https://nvd.nist.gov/vuln/detail/CVE-2024-5276

10	CVE-2024-30078	- Điểm CVSS: 8.8 (Cao) - Mô tả: Lỗ hổng tồn tại trên Wi-Fi Driver của Windows cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Windows 10. - Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.	https://nvd.nist.gov/vuln/detail/CVE-2024-30078
11	CVE-2024-37081	- Điểm CVSS: 7.8 (Cao) - Mô tả: Lỗ hổng cho phép đối tượng tấn công leo thang đặc quyền trên vCenter Server Appliance. - Ảnh hưởng: VMware vCenter Server. - Lỗ hổng đang bị khai thác trong thực tế.	https://nvd.nist.gov/vuln/detail/CVE-2024-37081
12	CVE-2024-3400	- Điểm CVSS: 10.0 (Nghiêm trọng) - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực hiện command injection, từ đó dẫn tới thực thi mã từ xa. - Ảnh hưởng: Palo Alto Networks PAN-OS. - Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.	https://nvd.nist.gov/vuln/detail/CVE-2024-3400

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. Cục An toàn thông tin đã phát hành Công văn số 1095/CATTT-NCSC ngày 14/6/2024 về việc cảnh báo nhóm APT "Mustang Panda" thực hiện chiến dịch tấn công nhằm vào Việt Nam.

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.



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 **6/2024**, Trung tâm NCSC phát hiện **11 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.

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:
- Như trên;
- 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 Chính sách xã hội;
- Ngân hàng Phát triển Việt Nam;
- Ngân hàng Hợp tác xã Việt Nam;
- 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;
- Cục trưởng (để b/c);
- Phó Cục trưởng Trần Đăng Khoa;
- Các phòng: ATHTTT, TT&HTQT;
- Trung tâm VNCERT/CC;
- Lưu: VT, NCSC.LTQ.

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

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 2024 của Cục An toàn thông tin)

TT	Website giả mạo	Ghi chú
1	https://shop[.]global-selling[.]top	Website giả mạo sàn TMĐT Amazon
2	https://vn156475p[.]com	Website giả mạo sàn TMĐT Amazon
3	https://vssid[.]govvvn[.]com	Website giả mạo Bảo hiểm Xã hội Việt Nam
4	https://vssidgov[.]com	Website giả mạo Bảo hiểm Xã hội Việt Nam
5	nappthe[.]vn	Website giả mạo Công Ty Cổ Phần Giải Trí Và Thể Thao Điện Tử Việt Nam
6	bachhoaxanhh[.]com	Website giả mạo Công ty cổ phần Thương mại Bách Hóa Xanh
7	https://nqsncoau[.]buzz/	Website giả mạo Cty tài chính tnhh ngân hàng việt nam thịnh vượng smbc
8	https://dienmayxanhctv24[.]com	Website giả mạo Điện máy xanh
9	https://thisinhthanhlich2024[.]com	Website giả mạo Facebook
10	https://binhchoncuocthivetranhsinhvien2024[.]weebly[.]com	Website giả mạo Facebook
11	https://duyetdonlazada[.]com	Website giả mạo sàn TMĐT Lazada
12	https://da8975[.]com	Website giả mạo sàn TMĐT Lazada

13	https://la5959[.]com	Website giả mạo sàn TMĐT Lazada
14	https://www[.]iazada[.]com/	Website giả mạo sàn TMĐT Lazada
15	moneytracking137[.]com	Website giả mạo Ngân Hàng TMCP Công Thương Việt Nam
16	https://tcbcanhan[.]com	Website giả mạo Ngân hàng TMCP Kỹ Thương Việt Nam
17	cskhcanhanhd[.]com	Website giả mạo Ngân hàng TMCP Phát triển Thành phố Hồ Chí Minh
18	hdbank[.]tructuyen-uudai-thekhachhang[.]com	Website giả mạo Ngân hàng TMCP Phát triển Thành phố Hồ Chí Minh
19	https://vnmcrd2s[.]online	Website giả mạo Ngân hàng TMCP Quân đội
20	https://mbdk99[.]com	Website giả mạo Ngân hàng TMCP Quân đội
21	https://www[.]dangnhaphoso[.]com	Website giả mạo Ngân hàng TMCP Quân đội
22	vib-care[.]com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
23	http://dich-vu-the-sat-vib[.]com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
24	https://vib[.]chamsockhachhang-uudai-tructuyenthe[.]com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
25	http://dich-vu-the-elite-vib[.]com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
26	https://vib[.]chamsockhachhang-tructuyenuudaithe[.]online	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
27	dich-vu-the-vvip-vib[.]com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
28	visa-vibbank[.]com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam

29	https://dich-vu-the-svip-vib[.]com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
30	https://nang-cap-ocare-vib[.]com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
31	vib-nangcap[.]com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
32	main-card-vib[.]com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
33	vib-up-the[.]shop	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
34	vib-cardnew[.]shop	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
35	vib-nang-the[.]com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
36	nang-cap-the-vcare-vib[.]com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
37	nang-cap-qcare-vib[.]com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
38	vib-solution[.]shop	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
39	https://tpbank[.]chamsockhachhang-uudaithe-thang6[.]com	Website giả mạo Ngân hàng TMCP Tiên Phong
40	www[.]vpbank[.]chamsockhachhang-uudaithecanhan-tructuyen[.]online	Website giả mạo Ngân hàng TMCP Việt Nam Thịnh Vượng
41	vpbank[.]uudai-tructuyen-chamsockhachhang-the[.]com[.]vn	Website giả mạo Ngân hàng TMCP Việt Nam Thịnh Vượng
42	https://www[.]tinchapshinhan[.]online	Website giả mạo Ngân hàng TNHH MTV Shinhan Việt Nam
43	https://sendotv[.]com	Website giả mạo sàn TMĐT Sendo
44	https://sp75193p[.]com	Website giả mạo sàn TMĐT Shopee
45	https://sp1663p[.]com	Website giả mạo sàn TMĐT Shopee

46	https://www[.]vn999mall[.]vip	Website giả mạo sàn TMĐT Shopee
47	https://sp1776p[.]com	Website giả mạo sàn TMĐT Shopee
48	sp7335p[.]com	Website giả mạo sàn TMĐT Shopee
49	https://vnc63661s[.]com	Website giả mạo sàn TMĐT Shopee
50	https://www[.]seleeashopee[.]com	Website giả mạo sàn TMĐT Shopee
51	https://www[.]thanhtrapcrt[.]online	Website giả mạo Thanh tra Chính phủ
52	https://fajiafu50[.]com	Website giả mạo sàn TMĐT Tiki
53	https://vntiki1[.]com	Website giả mạo sàn TMĐT Tiki
54	https://tdkt00[.]com	Website giả mạo sàn TMĐT Tiki
55	https://zla653[.]top	Website giả mạo sàn TMĐT Tiki
56	https://tdkt04[.]com	Website giả mạo sàn TMĐT Tiki
57	https://s2rjtiki[.]com	Website giả mạo sàn TMĐT Tiki
58	https://k2rjtiki[.]com	Website giả mạo sàn TMĐT Tiki
59	https://sh2tiki[.]com	Website giả mạo sàn TMĐT Tiki
60	https://tdkt06[.]com	Website giả mạo sàn TMĐT Tiki
61	https://fajiafu30[.]com/	Website giả mạo sàn TMĐT Tiki
62	https://viettlot135p[.]com	Website giả mạo Vietlott

63	Giaodichquoctes[.]com	Website giả mạo Western Union
64	https://giaodichquoctes[.]vercel[.]app	Website giả mạo Western Union
65	https://giaodichquoctes[.]com	Website giả mạo Western Union
66	https://nhantienquoctev3[.]vercel[.]app/	Website giả mạo Western Union
67	https://chuyentienquoctenhanh[.]vercel[.]app/	Website giả mạo Western Union
68	chuyentienquocte1313[.]vercel[.]app	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 2024 của Cục An toàn thông tin)

TT	Mã điểm yếu/ lỗ hổng	SL máy bị ảnh hưởng	Ghi chú
1	CVE-2022-26809	15025	https://nvd.nist.gov/vuln/detail/ CVE-2022-26809
2	CVE-2024-5499	7966	https://nvd.nist.gov/vuln/detail/ CVE-2024-5499
3	CVE-2024-5847	7649	https://nvd.nist.gov/vuln/detail/ CVE-2024-5847
4	CVE-2024-6103	7034	https://nvd.nist.gov/vuln/detail/ CVE-2024-6103
5	CVE-2023-21716	6613	https://nvd.nist.gov/vuln/detail/ CVE-2023-21716
6	CVE-2024-5274	5412	https://nvd.nist.gov/vuln/detail/ CVE-2024-5274
7	CVE-2024-29072	4146	https://nvd.nist.gov/vuln/detail/ CVE-2024-29072
8	CVE-2024-35265	4081	https://nvd.nist.gov/vuln/detail/ CVE-2024-35265
9	CVE-2024-5841	2566	https://nvd.nist.gov/vuln/detail/ CVE-2024-5841
10	CVE-2024-5701	2122	https://nvd.nist.gov/vuln/detail/ CVE-2024-5701

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	89.44.197.74	APT Crimson Palace
2	195.123.247.50	
3	185.195.237.121	
4	195.123.245.79	
5	msudapis.info	
6	185.167.116.30	
7	139.162.18.97	
8	64.176.50.42	
9	139.180.217.105	
10	198.13.47.158	
11	scancenter.trendrealtime.com	
12	172.67.130.71	
13	104.21.3.57	
14	associate.feedfoodconcerning.info	
15	154.39.137.29	
16	associate.freeonlinelearning.com	

17	message.ooguy.com	
18	158.247.241.188	
19	45.130.229.181	
20	185.195.237.123	
21	45.90.58.103	
22	185.82.217.164	
23	associate.freeonlinelearningtech.com	
24	147.139.47.141	
25	91.220.202.143	
26	146.190.93.250	
27	www.googlespeedtest33.com	
28	185.201.8.187	
29	hxxp://mega.vlvlvlvl[.]site/Vanban_8647.PDF_update.hta	APT Mustang Panda
30	hxxp://mega.vlvlvlvl[.]site/HPCustPartUI.dll	
31	hxxp://payment.tripadviso[.]online/tempdata.dat	
32	hxxp://megacybernews[.]com/newrun.ps1	
33	hxxp://megacybernews[.]com/stage2.2.ps1	
34	hxxp://megacybernews[.]com/book.dll	
35	hxxp://megacybernews[.]com/wwlib.dll	

36	payment.tripadviso[.]online	
37	megacybernews[.]com	
38	hxxp://mega.vlvlvlvl[.]site/HP.exe	
39	hxxp://mega.vlvlvlvl[.]site/Vanban_8647.PDF.ps1	
40	hxxp://vibm[.]vn/init.txt	
41	hxxp://megacybernews[.]com/getdata.ps1	
42	hxxp://megacybernews[.]com/checkin.php	
43	hxxp://megacybernews[.]com/unikey.exe	
44	mega.vlvlvlvl[.]site	
45	vibm[.]vn	
46	8.222.218.20	APT UNC3886
47	8.222.216.144	
48	8.219.131.77	
49	8.219.0.112	
50	8.210.75.218	
51	8.210.103.134	
52	47.252.54.82	
53	47.251.46.35	
54	47.246.68.13	

55	47.243.116.155	APT UNC3886
56	47.241.56.157	
57	165.154.134.40	
58	207.246.64.38	
59	149.28.122.119	
60	155.138.161.47	
61	154.216.2.149	
62	103.232.86.217	
63	103.232.86.210	
64	103.232.86.209	
65	58.64.204.165	
66	58.64.204.142	
67	58.64.204.139	
68	165.154.7.145	
69	165.154.135.108	
70	152.32.231.251	
71	152.32.205.208	
72	152.32.144.15	
73	152.32.129.162	

74	123.58.207.86	
75	123.58.196.34	
76	118.193.63.40	
77	118.193.61.71	
78	118.193.61.178	
79	45.77.106.183	
80	45.32.252.98	

Phụ lục IV

DANH SÁCH CÁC ĐƠN VỊ CÓ ĐỊA CHỈ IP NẰM TRONG MẠNG BOTNET

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

1. Danh sách Bộ/Ngành

TT	Tên đơn vị	Số lượng IP botnet tháng 05/2024	Số lượng IP botnet tháng 06/2024	Loại mã độc/botnet
1	Bảo hiểm Xã hội Việt Nam	0	1	Andromeda

2. Danh sách Tỉnh/thành

STT	Tên đơn vị	Số lượng IP botnet tháng 05/2024	Số lượng IP botnet tháng 06/2024	Ghi chú
1	Lai Châu	4	6	Andromeda
2	Hà Nam	3	3	Andromeda
3	Nam Định	1	2	Andromeda
4	Thanh Hóa	1	2	Andromeda
5	Thái Bình	2	1	Andromeda
6	Gia Lai	1	1	Andromeda
7	Hà Nội	1	1	Andromeda
8	Lạng Sơn	1	1	Andromeda
9	Ninh Bình	0	1	Andromeda
10	Kon Tum	0	1	Andromeda
11	Hà Giang	1	0	

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 2024 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 30/06/2024)
1	Bộ Công Thương	09/08/2020	30/06/2024
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	30/06/2024
5	Bộ Khoa học và Công nghệ	19/11/2020	25/06/2024
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**	**Không nhận được dữ liệu chia sẻ**
8	Bộ Nội vụ	30/07/2020	30/06/2024
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	30/06/2024
11	**Bộ Tài nguyên và Môi trường**	**03/10/2020**	**Không nhận được dữ liệu chia sẻ**
12	Bộ Thông tin và Truyền thông	11/02/2022	30/06/2024
13	Bộ Tư pháp	18/03/2023	30/06/2024
14	**Bộ Văn hóa, Thể thao và Du lịch**	**20/06/2020**	**Không nhận được dữ liệu chia sẻ**
15	Bộ Xây Dựng	23/07/2020	30/06/2024
16	**Bộ Y tế**	**17/07/2020**	**Không nhận được dữ liệu chia sẻ**

17	Ngân hàng Nhà nước Việt Nam	02/07/2020	30/06/2024
18	**Thanh tra Chính phủ**	**10/11/2020**	**Không nhận được dữ liệu chia sẻ**
19	Ủy ban Dân tộc	08/10/2020	30/06/2024
20	**Văn phòng Chính phủ**	**22/09/2020**	**Không nhận được dữ liệu chia sẻ**
21	Bảo Hiểm Xã Hội	08/11/2020	30/06/2024
22	Đài Truyền hình Việt Nam	14/09/2020	30/06/2024
23	Viện Hàn Lâm KHCN	22/09/2020	30/06/2024
24	**Kiểm toán Nhà nước Việt Nam**	**09/03/2021**	**Không nhận được dữ liệu chia sẻ**

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 30/06/2024)
1	An Giang	30/09/2020	30/06/2024
2	Bắc Giang	21/08/2020	30/06/2024
3	Bắc Kạn	01/09/2020	30/06/2024
4	**Bạc Liêu**	**09/10/2020**	**Không nhận được dữ liệu chia sẻ**
5	Bắc Ninh	23/07/2020	30/06/2024
6	Bà Rịa - Vũng Tàu	20/07/2020	30/06/2024
7	Bến Tre	10/08/2020	30/06/2024
8	Bình Định	05/06/2020	30/06/2024
9	Bình Dương	24/04/2020	30/06/2024
10	Bình Phước	23/04/2020	30/06/2024
11	Bình Thuận	31/08/2020	30/06/2024
12	Cà Mau	15/05/2020	29/06/2024
13	Cần Thơ	13/04/2020	30/06/2024
14	Cao Bằng	14/08/2020	30/06/2024
15	Đắk Lắk	17/06/2020	30/06/2024
16	Đắk Nông	31/08/2020	30/06/2024
17	Đà Nẵng	09/06/2020	28/06/2024
18	Điện Biên	02/06/2020	30/06/2024
19	Đồng Nai	15/06/2020	30/06/2024
20	Đồng Tháp	14/07/2020	30/06/2024
21	Gia Lai	14/09/2020	30/06/2024
22	Hà Giang	18/08/2020	30/06/2024
23	**Hải Dương**	**04/09/2020**	**Không nhận được dữ liệu chia sẻ**
24	Hải Phòng	28/07/2020	30/06/2024
25	Hà Nam	22/09/2020	30/06/2024
26	Hà Nội	30/06/2020	25/06/2024

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

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

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 2024 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 06/2024	Ghi chú
1	Bộ Công Thương	193	
2	**Bộ Giáo dục và Đào tạo**	**0**	**Chưa chia sẻ**
3	Bộ Giao thông vận tải	82	
4	Bộ Kế hoạch và Đầu tư	1178	
5	Bộ Khoa học và Công nghệ	366	
6	**Bộ Lao động - Thương Binh và Xã hội**	**0**	**Mất kết nối 01 tháng trở lên**
7	Bộ Ngoại giao	10	
8	Bộ Nội vụ	452	
9	**Bộ Nông nghiệp và Phát triển nông thôn**	**0**	**Chưa chia sẻ**
10	Bộ Tài chính	265	
11	Bộ Tài nguyên và Môi trường	55	
12	Bộ Thông tin và Truyền thông	224	
13	Bộ Tư pháp	7606	
14	Bộ Văn hóa, Thể thao và Du lịch	17	
15	Bộ Xây Dựng	25	
16	Bộ Y tế	53	

17	Ngân hàng Nhà nước Việt Nam	3179	
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	3	
22	Bảo Hiểm Xã Hội	14550	
23	Đài tiếng nói Việt Nam	14	
24	Đài Truyền hình Việt Nam	184	
25	Thông tấn xã Việt Nam	1629	
26	Viện Hàn Lâm KHCN	115	
27	Viện Hàn Lâm KHXH	153	
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 06/2024	Ghi chú
1	An Giang	472	
2	Bắc Giang	1070	
3	Bắc Kạn	3526	
4	Bạc Liêu	1930	
5	Bắc Ninh	1782	
6	Bà Rịa - Vũng Tàu	38085	
7	Bến Tre	37	
8	Bình Định	164	
9	Bình Dương	8567	
10	Bình Phước	3796	
11	Bình Thuận	3346	
12	Cà Mau	1150	
13	Cần Thơ	1502	
14	Cao Bằng	1166	
15	Đắk Lắk	5203	
16	Đắk Nông	1245	

17	Đà Nẵng	47493	
18	Điện Biên	4046	
19	Đồng Nai	4218	
20	Đồng Tháp	8430	
21	Gia Lai	20	
22	Hà Giang	14	
23	Hải Dương	2156	
24	Hải Phòng	42	
25	Hà Nam	919	
26	Hà Nội	6239	
27	Hà Tĩnh	2112	
28	Hòa Bình	859	
29	Hồ Chí Minh	10013	
30	Hậu Giang	972	
31	Hưng Yên	546	
32	Khánh Hòa	2926	
33	Kiên Giang	3516	
34	Kon Tum	4698	

35	Lai Châu	33	
36	Lâm Đồng	215	
37	Lạng Sơn	332	
38	Lào Cai	3	
39	Long An	2690	
40	Nam Định	43	
41	Nghệ An	5120	
42	Ninh Bình	147	
43	Ninh Thuận	907	
44	Phú Thọ	10	
45	Phú Yên	128	
46	Quảng Bình	2608	
47	Quảng Nam	242	
48	Quảng Ngãi	3625	
49	**Quảng Ninh**	**0**	**Mất kết nối 01 tháng trở lên**
50	Quảng Trị	293	
51	Sóc Trăng	36	
52	Sơn La	4188	

53	Tây Ninh	1474	
54	Thái Bình	3650	
55	Thái Nguyên	2057	
56	Thanh Hóa	1429	
57	Thừa Thiên Huế	6017	
58	Tiền Giang	52775	
59	Trà Vinh	1284	
60	Tuyên Quang	3382	
61	Vĩnh Long	3259	
62	Vĩnh Phúc	11668	
63	Yên Bái	1085	

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-CATTT 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).