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: 22 /BC-CATTT

Hà Nội, ngày 21 tháng 11 năm 2024

BÁO CÁO AN TOÀN THÔNG TIN MẠNG VIỆT NAM
(Tháng 10/2024)

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 **10/2024**, 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 **10/2024**, 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 30/11/2024.**

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 10/2024.

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-10-2024.244/

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/

Văn bản số 2130/CATTT-NCSC về việc Cảnh báo về lỗ hổng an toàn thông tin tồn tại trên sản phẩm Oracle WebLogic Server phát hành ngày 23/10/2024.

Thông tin chi tiết tại: https://khonggianmang.vn/alert/canh-bao-ve-lo-hong-an-toan-thong-tin-trong-san-pham-cua-oracle-web-logic-server.250

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 **10/2024** 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 **73/87** đơn vị có kết nối chia sẻ dữ liệu tương đối đầy đủ, **14/87** 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.*

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 **10/2024** 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 **80/88 đơn vị** có kết nối thường xuyên. Trong các đơn vị kết nối thường xuyên có **80/80 đơn vị** chia sẻ về hệ điều hành các máy **(tổng số máy là 312.937)**.

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, 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 **125.448 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 **5.942 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 **10/2024**, hệ thống của NCSC đã phát hiện **49 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 **56.496** 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 **10/2024**, 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 10/2024:

TT	Mã điểm yếu/lỗ hổng	Mô tả	Ghi chú
1	CVE-2024-9164	- Điểm CVSS: 9.6 (Nghiêm trọng) - Mô tả: Lỗ hổng cho phép đối tượng tấn công truy cập và thực hiện các hành vi trái phép. - Ảnh hưởng: GitLab. - Lỗ hổng chưa có mã khai thác và đang bị khai thác trong thực tế.	https://nvd.nist.gov/vuln/detail/CVE-2024-9164
2	CVE-2024-38178	- 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.	https://nvd.nist.gov/vuln/detail/CVE-2024-38178

		- Ảnh hưởng: Microsoft. - Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.	
3	CVE-2021-4043	- Điểm CVSS: 5.5 (Trung bình) - Mô tả: Lỗ hổng cho phép đối tượng tấn công truy cập và thực hiện các hành vi trái phép. - Ảnh hưởng: Gpac. - Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.	https://nvd.nist.gov/vuln/detail/CVE-2021-4043
4	CVE-2024-3080	- Điểm CVSS: 9.8 (Nghiêm trọng) - Mô tả: Lỗ hổng cho phép đối tượng tấn công truy cập và thực hiện các hành vi. - Ảnh hưởng: ASUS router. - Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.	https://nvd.nist.gov/vuln/detail/CVE-2024-3080
5	CVE-2024-9441	- Điểm CVSS: 9.8 (Nghiêm trọng) - Mô tả: Lỗ hổng cho phép đối tượng tấn công. - Ảnh hưởng: Access Control - Linear eMerge e3-Series. - Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.	https://nvd.nist.gov/vuln/detail/CVE-2024-9441
6	CVE-2024-35202	- Điểm CVSS: 7.5 (Cao) - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ. - Ảnh hưởng: BitCoin Core. - Lỗ hổng chưa có mã khai thác và chưa bị khai thác trong thực tế.	https://nvd.nist.gov/vuln/detail/CVE-2024-35202
7	CVE-2024-47575	- Điểm CVSS: 9.8 (Nghiêm trọng) - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: FortiManager. - Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.	https://nvd.nist.gov/vuln/detail/CVE-2024-47575

8	CVE-2024-45409	- Điểm CVSS: 9.8 (Nghiêm trọng) - Mô tả: Lỗ hổng cho phép đối tượng tấn công truy cập và thực thi các hành vi trái phép. - Ảnh hưởng: Ruby SAML library. - Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.	https://nvd.nist.gov/vuln/detail/CVE-2024-45409
9	CVE-2024-45519	- Điểm CVSS: 9.8 (Nghiêm trọng) - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Zimbra. - Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.	https://nvd.nist.gov/vuln/detail/CVE-2024-45519
10	CVE-2024-9463	- Điểm CVSS: 7.5 (Cao) - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Palo Alto Networks Expedition. - Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.	https://nvd.nist.gov/vuln/detail/CVE-2024-9463
11	CVE-2024-28000	- Điểm CVSS: 9.8 (Nghiêm trọng) - Mô tả: Lỗ hổng cho phép đối tượng tấn công leo thang đặc quyền. - Ảnh hưởng: LiteSpeed Technologies LiteSpeed Cache. - Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.	https://nvd.nist.gov/vuln/detail/CVE-2024-28000
12	CVE-2024-37383	- Điểm CVSS: 6.1 (Trung bình) - Mô tả: Lỗ hổng cho phép đối tượng tấn công khai thác lỗi XSS. - Ảnh hưởng: Roundcube Webmail. - Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.	https://nvd.nist.gov/vuln/detail/CVE-2024-37383

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 2130/CATTT-NCSC về việc Cảnh báo về lỗ hổng an toàn thông tin tồn tại trên sản phẩm Oracle WebLogic Server phát hành ngày 23/10/2024.

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 **10/2024**, Trung tâm NCSC phát hiện **16 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 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

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

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 2024 của Cục An toàn thông tin)

TT	Website giả mạo	Ghi chú
1	https://amazoul[.]xyz	Website giả mạo sàn TMĐT Amazon
2	amazoul[.]site	Website giả mạo sàn TMĐT Amazon
3	amazonl0[.]com	Website giả mạo sàn TMĐT Amazon
4	amazoni2[.]com	Website giả mạo sàn TMĐT Amazon
5	www[.]ccty-ghtk[.]com	Website giả mạo Công ty cổ phần giao hàng tiết kiệm
6	dichvugiaohangtietkiem[.]com	Website giả mạo Công ty cổ phần giao hàng tiết kiệm
7	ghtk247[.]com	Website giả mạo Công ty cổ phần giao hàng tiết kiệm
8	giaohangtietkiemvn[.]website	Website giả mạo Công ty cổ phần giao hàng tiết kiệm
9	chats-ghtkvn[.]com	Website giả mạo Công ty cổ phần giao hàng tiết kiệm
10	giaohangtietkiem666[.]com	Website giả mạo Công ty cổ phần giao hàng tiết kiệm
11	soyte[.]cc	Website giả mạo Dịch vụ công quốc gia
12	dichvucong[.]ccbcavn[.]cc	Website giả mạo Dịch vụ công quốc gia
13	vietcp[.]com	Website giả mạo Dịch vụ công Quốc Gia

14	dichvudienmay-xanh[.]online	Website giả mạo Điện máy xanh
15	dienmayxanhcenter[.]vn	Website giả mạo Điện máy xanh
16	dienlanhdienmayxanhvn[.]com	Website giả mạo Điện máy xanh
17	https://fasebook[.]com[.]vn	Website giả mạo Facebook
18	hanoixanh2024[.]weebly[.]com	Website giả mạo Facebook
19	thuongmai-dientu[.]com	Website giả mạo sàn TMĐT Lazada
20	momoshopvip[.]com	Website giả mạo MoMo
21	acb[.]chamsockhachhang-the-tructuyen-thang9[.]com[.]vn	Website giả mạo Ngân hàng TMCP Á Châu
22	https://acb[.]chamsockhachhang-uudai-tructuyen-thang10[.]com[.]vn	Website giả mạo Ngân hàng TMCP Á Châu
23	https://acb[.]uudauthekhachhanh-tructuyen-thang10[.]com[.]vn	Website giả mạo Ngân hàng TMCP Á Châu
24	https://acb[.]chamsocthe-uudaikhachhang[.]online	Website giả mạo Ngân hàng TMCP Á Châu
25	acb[.]uudaikhachhang-chamsocthetructuyen[.]com	Website giả mạo Ngân hàng TMCP Á Châu
26	www[.]acb[.]uudaikhachhang-tructuyen-the[.]com[.]vn	Website giả mạo Ngân hàng TMCP Á Châu
27	www[.]acb[.]chamsocthe-uudaikhachhang-tructuyen[.]com	Website giả mạo Ngân hàng TMCP Á Châu
28	acb[.]chamsocthe-uudaitructuyen[.]com[.]vn	Website giả mạo Ngân hàng TMCP Á Châu
29	acb[.]chamsocthe-uudaikhachhang-thang10[.]com[.]vn	Website giả mạo Ngân hàng TMCP Á Châu

30	acb[.]chamsockhachhang-uudaithetructuyen-thang10[.]com[.]vn	Website giả mạo Ngân hàng TMCP Á Châu
31	www[.]acb[.]chamsocthe-uudai-tructuyen-thang10[.]com[.]vn	Website giả mạo Ngân hàng TMCP Á Châu
32	cms[.]mb6098[.]com	Website giả mạo Ngân hàng TMCP Quân đội
33	vpbank[.]uudaikhachhang-chamsocthetructuyen[.]com[.]vn	Website giả mạo Ngân hàng TMCP Việt Nam Thịnh Vượng
34	shinhan[.]chamsocthe-uudaikhachhang[.]com	Website giả mạo Ngân hàng TNHH MTV Shinhan Việt Nam
35	tiki886[.]vip	Website giả mạo sàn TMĐT Sendo
36	sendo1[.]com	Website giả mạo sàn TMĐT Sendo
37	https://www[.]tb88789[.]com	Website giả mạo sàn TMĐT Shopee
38	https://www[.]sp7588p[.]com	Website giả mạo sàn TMĐT Shopee
39	s[.]shopee[.]vn	Website giả mạo sàn TMĐT Shopee
40	sp5583p[.]com	Website giả mạo sàn TMĐT Shopee
41	www[.]evnnpcs[.]com	Website giả mạo Tập đoàn Điện lực Việt Nam (EVN)
42	evn[.]brvgov[.]com	Website giả mạo Tập đoàn Điện lực Việt Nam (EVN)
43	korshoptiktok[.]com	Website giả mạo Tik tok
44	www[.]tikifreeship[.]cc	Website giả mạo sàn TMĐT Tiki
45	topcvvn[.]com	Website giả mạo Top CV

46	https://jetkingncsc[.]online	Website giả mạo Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC)
47	chinhphu[.]thongtincancuoc[.]com	Website giả mạo Văn phòng Chính phủ
48	vneid[.]vieegovn[.]cc	Website giả mạo VNeID
49	https://nhantienquoctejp17ww[.]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	14867	https://nvd.nist.gov/vuln/detail/ CVE-2022-26809
2	CVE-2023-21716	6593	https://nvd.nist.gov/vuln/detail/ CVE-2023-21716
3	CVE-2024-9256	2864	https://nvd.nist.gov/vuln/detail/ CVE-2024-9256
4	CVE-2024-6197	2351	https://nvd.nist.gov/vuln/detail/ CVE-2024-6197
5	CVE-2024-9936	2200	https://nvd.nist.gov/vuln/detail/ CVE-2024-9936
6	CVE-2023-40477	2017	https://nvd.nist.gov/vuln/detail/ CVE-2024-40477
7	CVE-2024-9603	1421	https://nvd.nist.gov/vuln/detail/ CVE-2021-9603
8	CVE-2024-10231	1322	https://nvd.nist.gov/vuln/detail/ CVE-2024-10231
9	CVE-2024-9966	1291	https://nvd.nist.gov/vuln/detail/ CVE-2024-9966
10	CVE-2024-9403	1284	https://nvd.nist.gov/vuln/detail/ CVE-2021-9403

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	104.21.81[.]233	Nhóm APT **"CeranaKeeper"**
2	172.67.165[.]197	
3	103.245.165[.]237	
4	103.27.202[.]185	
5	103.27.202[.]185	
6	www.toptipvideo[.]com	
7	inly5sf[.]com	
8	dljmp2p[.]com	
9	www.dl6yfsl[.]com	
10	www.uvfr4ep[.]com	
11	95.164.17[.]24	Nhóm **CL-STA-0240**
12	000b4a77b1905cabdb59d2b576f6da1b2ef55a0258004e4a9e290e9f41fb6923	
13	0f5f0a3ac843df675168f82021c24180ea22f764f87f82f9f77fe8f0ba0b7132	
14	36cac29ff3c503c2123514ea903836d5ad81067508a8e16f7947e3e675a08670	
15	fd9e8fcc5bda88870b12b47cbb1cc8775ccff285f980c4a2b683463b26e36bf0	
16	9e3a9dbf10793a27361b3cef4d2c87dbd3662646f4470e5242074df4cb96c6b4	

17	185.235.241[.]208	
18	9abf6b93eafb797a3556bea1fe8a3b7311d2864d5a9a3687fce84bc1ec4a428c	
19	d801ad1beeab3500c65434da51326d7648a3c54923d794b2411b7b6a2960f31e	
20	de6f9e9e2ce58a604fe22a9d42144191cfc90b4e0048dffcc69d696826ff7170	
21	0621d37818c35e2557fdd8a729e50ea662ba518df8ca61a44cc3add5c6deb3cd	
22	d5c0b89e1dfbe9f5e5b2c3f745af895a36adf772f0b72a22052ae6dfa045cea6	
23	126-com[.]live	Nhóm APT **SideWinder**
24	alit[.]live	
25	asyn[.]info	
26	cnsa-gov[.]org	
27	condet[.]org	
28	decoty[.]tech	
29	detru[.]info	
30	dinfed[.]co	
31	direct888[.]net	
32	donwload-file[.]com	
33	dowmload[.]net	
34	downloadabledocx[.]com	
35	e1ix[.]mov	

36	fia-gov[.]net	Nhóm APT **SideWinder**
37	govpk[.]net	
38	healththebest[.]com	
39	kretic[.]info	
40	mfa-gov[.]net	
41	mfagov[.]org	
42	mod-gov-pk[.]live	
43	moittpk[.]net	
44	nactagovpk[.]org	
45	updtesession[.]online	
46	tni-mil[.]com	
47	u1x[.]co	
48	163inc[.]com	
49	aliyum[.]tech	
50	ausibedu[.]org	
51	colot[.]info	
52	conft[.]live	
53	defenec[.]net	
54	dgps-govpk[.]co	

55	dirctt88[.]co	Nhóm APT **SideWinder**
56	direct88[.]co	
57	donwloaded[.]com	
58	downld[.]net	
59	dynat[.]tech	
60	e1x[.]tech	
61	gov-govpk[.]info	
62	grouit[.]tech	
63	jmicc[.]xyz	
64	lforvk[.]com	
65	mfa-govt[.]net	
66	mfas[.]pro	
67	mofa[.]email	
68	moittpk[.]org	
69	navy-mil[.]co	
70	nopler[.]live	
71	ntcpk[.]info	
72	numzy[.]net	
73	afmat[.]tech	

74	aliyumm[.]tech	Nhóm APT **SideWinder**
75	bol-south[.]org	
76	comptes[.]tech	
77	dafpak[.]org	
78	defpak[.]org	
79	dgps-govpk[.]com	
80	dirctt88[.]net	
81	directt888[.]com	
82	donwloaded[.]net	
83	download-file[.]net	
84	dytt88[.]org	
85	fia-gov[.]com	
86	govpk[.]info	
87	gtrec[.]info	
88	kernet[.]info	
89	mfa-gov[.]info	
90	mfacom[.]org	
91	mitlec[.]site	
92	mofagovs[.]org	

93	mshealthcheck[.]live	Nhóm APT **SideWinder**
94	newmofa[.]com	
95	ntcpak[.]live	
96	ntcpk[.]net	
97	nventic[.]info	
98	newoutlook[.]live	
99	ntcpak[.]org	
100	numpy[.]info	
101	office-drive[.]live	
102	paknavy-govpk[.]info	
103	pdfrdr-update[.]info	
104	pmd-office[.]org	
105	shipping-policy[.]info	
106	tazze[.]co	
107	tsinghua-edu[.]tech	
108	ujsen[.]net	
109	widge[.]info	
110	pafgovt[.]com	
111	paknavy-govpk[.]net	

112	pmd-office[.]com	
113	ptcl-net[.]com	
114	sjfu-edu[.]co	
115	tex-ideas[.]info	
116	tumet[.]info	
117	update-govpk[.]co	
118	paknavy-gov[.]org	
119	pdfrdr-update[.]com	
120	pmd-office[.]live	
121	scrabt[.]tech	
122	support-update[.]info	
123	B2DC7AEC2C6D2FFA28219AC288E4750C	Nhóm APT **Lazarus Group**
124	7353AB9670133468081305BD442F7691CF2F2C1136F09D9508400546C417833A	
125	7F28AD5EE9966410B15CA85B7FACB70088A17C5F	
126	detankzone[.]com	
127	E5DA4AB6366C5690DFD1BB386C7FE0C78F6ED54F	
128	8312E556C4EEC999204368D69BA91BF4	
129	59A37D7D2BF4CFFE31407EDD286A811D9600B68FE757829E30DA4394AB65A4CC	
130	ccwaterfall[.]com	

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 09/2024	Số lượng IP botnet tháng 10/2024	Loại mã độc/botnet
1	Bộ Khoa học và Công nghệ	2	2	Andromeda
2	Đài Tiếng nói Việt Nam	1	1	Andromeda

2. Danh sách Tỉnh/thành

STT	Tên đơn vị	Số lượng IP botnet tháng 09/2024	Số lượng IP botnet tháng 10/2024	Ghi chú
1	Lai Châu	5	3	Andromeda
2	Thái Bình	2	2	Andromeda
3	Thanh Hóa	2	2	Andromeda
4	An Giang	1	1	Andromeda
5	Bà Rịa Vũng Tàu	2	1	Andromeda
6	Cao Bằng	0	1	Andromeda
7	Điện Biên	2	1	Andromeda
8	Hà Nội	1	1	Andromeda
9	Lâm Đồng	1	1	Andromeda
10	Lào Cai	0	1	Andromeda

11	Nam Định	1	1	Andromeda
12	Ninh Bình	1	1	Andromeda
13	Quảng Ninh	1	1	Andromeda
14	Cần Thơ	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 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 31/10/2024)
1	Bộ Công Thương	09/08/2020	31/10/2024
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	02/10/2024
5	Bộ Khoa học và Công nghệ	19/11/2020	31/10/2024
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	31/10/2024
8	Bộ Nội vụ	30/07/2020	31/10/2024
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	31/10/2024
11	Bộ Tài nguyên và Môi trường	03/10/2020	31/10/2024
12	Bộ Thông tin và Truyền thông	11/02/2022	31/10/2024
13	Bộ Tư pháp	18/03/2023	31/10/2024
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	31/10/2024
16	**Bộ Y tế**	**17/07/2020**	**Không nhận được dữ liệu chia sẻ**
17	Ngân hàng Nhà nước Việt Nam	02/07/2020	31/10/2024

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

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

27	Hà Tĩnh	06/10/2020	31/10/2024
28	Hòa Bình	13/05/2020	31/10/2024
29	Hồ Chí Minh	26/06/2020	31/10/2024
30	Hậu Giang	02/10/2020	03/10/2024
31	Hưng Yên	22/05/2020	31/10/2024
32	Khánh Hòa	21/09/2020	31/10/2024
33	Kiên Giang	24/09/2020	31/10/2024
34	Kon Tum	28/09/2020	31/10/2024
35	Lai Châu	26/09/2020	30/10/2024
36	Lâm Đồng	22/10/2020	20/10/2024
37	Lạng Sơn	08/10/2020	31/10/2024
38	Lào Cai	09/07/2020	31/10/2024
39	Long An	22/07/2020	31/10/2024
40	Nam Định	21/09/2020	31/10/2024
41	Nghệ An	09/09/2020	31/10/2024
42	Ninh Bình	28/07/2020	31/10/2024
43	Ninh Thuận	01/09/2020	31/10/2024
44	**Phú Thọ**	**01/10/2020**	**Không nhận được dữ liệu chia sẻ**
45	Phú Yên	30/11/2020	31/10/2024
46	Quảng Bình	01/07/2020	31/10/2024
47	**Quảng Nam**	**14/09/2020**	**Không nhận được dữ liệu chia sẻ**
48	Quảng Ngãi	12/08/2020	31/10/2024
49	Quảng Ninh	12/09/2020	30/10/2024
50	Quảng Trị	24/12/2020	31/10/2024
51	**Sóc Trăng**	**12/08/2020**	**Không nhận được dữ liệu chia sẻ**
52	Sơn La	13/07/2020	31/10/2024
53	**Tây Ninh**	**08/07/2020**	**Không nhận được dữ liệu chia sẻ**
54	Thái Bình	25/06/2020	31/10/2024
55	**Thái Nguyên**	**19/11/2020**	**Không nhận được dữ liệu chia sẻ**

56	Thanh Hóa	29/09/2020	31/10/2024
57	Thừa Thiên Huế	29/07/2020	31/10/2024
58	Tiền Giang	24/09/2020	31/10/2024
59	Trà Vinh	29/07/2020	31/10/2024
60	Tuyên Quang	19/11/2020	30/10/2024
61	Vĩnh Long	25/06/2020	31/10/2024
62	Vĩnh Phúc	30/06/2020	31/10/2024
63	Yên Bái	26/08/2020	31/10/2024

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 10/2024	Ghi chú
1	Bộ Công Thương	198	
2	**Bộ Giáo dục và Đào tạo**	**0**	**Chưa chia sẻ**
3	Bộ Giao thông vận tải	88	
4	Bộ Kế hoạch và Đầu tư	1198	
5	Bộ Khoa học và Công nghệ	411	
6	**Bộ Lao động - Thương Binh và Xã hội**	**0**	**Mất kết nối 01 tháng trở lên**
7	**Bộ Ngoại giao**	**0**	**Mất kết nối 01 tháng trở lên**
8	Bộ Nội vụ	440	
9	**Bộ Nông nghiệp và Phát triển nông thôn**	**0**	**Chưa chia sẻ**
10	Bộ Tài chính	295	
11	Bộ Tài nguyên và Môi trường	1923	
12	Bộ Thông tin và Truyền thông	294	
13	Bộ Tư pháp	896	
14	Bộ Văn hóa, Thể thao và Du lịch	64	
15	Bộ Xây Dựng	32	
16	Bộ Y tế	77	

17	Ngân hàng Nhà nước Việt Nam	3549	
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	1	
22	Bảo Hiểm Xã Hội	15066	
23	Đài tiếng nói Việt Nam	10	
24	Đài Truyền hình Việt Nam	179	
25	Thông tấn xã Việt Nam	1589	
26	Viện Hàn Lâm KHCN	113	
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 10/2024	Ghi chú
1	An Giang	440	
2	Bắc Giang	7118	
3	Bắc Kạn	2881	
4	Bạc Liêu	1905	
5	Bắc Ninh	1679	
6	Bà Rịa - Vũng Tàu	24260	
7	Bến Tre	1569	
8	Bình Định	169	
9	Bình Dương	1775	
10	Bình Phước	4619	
11	Bình Thuận	3655	
12	Cà Mau	1748	
13	Cần Thơ	1339	
14	Cao Bằng	1287	
15	Đắk Lắk	5205	
16	Đắk Nông	1141	

17	Đà Nẵng	51839	
18	Điện Biên	3938	
19	Đồng Nai	4778	
20	Đồng Tháp	7124	
21	Gia Lai	19	
22	Hà Giang	14	
23	**Hải Dương**	**0**	**Mất kết nối 01 tháng trở lên**
24	Hải Phòng	4891	
25	Hà Nam	952	
26	Hà Nội	62322	
27	Hà Tĩnh	1960	
28	Hòa Bình	1167	
29	Hồ Chí Minh	1	
30	Hậu Giang	1201	
31	Hưng Yên	505	
32	Khánh Hòa	2907	
33	Kiên Giang	2277	
34	Kon Tum	5128	

35	Lai Châu	34	
36	Lâm Đồng	2712	
37	Lạng Sơn	317	
38	Lào Cai	2	
39	Long An	2922	
40	Nam Định	41	
41	Nghệ An	4979	
42	Ninh Bình	594	
43	Ninh Thuận	649	
44	Phú Thọ	11	
45	Phú Yên	153	
46	Quảng Bình	2486	
47	Quảng Nam	243	
48	Quảng Ngãi	3790	
49	**Quảng Ninh**	**0**	**Mất kết nối 01 tháng trở lên**
50	Quảng Trị	371	
51	Sóc Trăng	37	
52	Sơn La	3973	

53	Tây Ninh	1209	
54	Thái Bình	3332	
55	Thái Nguyên	2043	
56	Thanh Hóa	1492	
57	Thừa Thiên Huế	6927	
58	Tiền Giang	27300	
59	Trà Vinh	1317	
60	Tuyên Quang	3347	
61	Vĩnh Long	3441	
62	Vĩnh Phúc	17	
63	Yên Bái	962	

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).