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: 24 /BC-CATTT

Hà Nội, ngày 16 tháng 12 năm 2024

BÁO CÁO AN TOÀN THÔNG TIN MẠNG VIỆT NAM
(Tháng 11/2024)

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 **11/2024**, 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 **11/2024**, 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 25/12/2024.**

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 11/2024.

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-11-2024.253/

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 2448/CATTT-NCSC về việc Cảnh báo chiến dịch tấn công có chủ đích của nhóm APT Earth Estries phát hành ngày 22/11/2024.

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 **11/2024** 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.*

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 **11/2024** 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 **79/88 đơn vị** có kết nối thường xuyên. Trong các đơn vị kết nối thường xuyên có **79/79 đơn vị** chia sẻ về hệ điều hành các máy **(tổng số máy là 292.457)**.

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 **125.506 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 **11/2024**, hệ thống của NCSC đã phát hiện **77 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 **73.979** 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 **11/2024**, 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 11/2024:

TT	Mã điểm yếu/lỗ hổng	Mô tả	Ghi chú
1	CVE-2024-43451	- Điểm CVSS: 6.5 (Cao) - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực hiện tấn công giả mạo (Spoofing) - Ảnh hưởng: Windows - Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế	https://nvd.nist.gov/vuln/detail/CVE-2024-43451
2	CVE-2024-21287	- 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-2024-21287

		- Ảnh hưởng: Oracle Agile PLM Framework thuộc Oracle Supply Chain - Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế	
3	CVE-2024-11680	- Điểm CVSS: Chưa xác định - Mô tả: Lỗ hổng cho phép đối tượng tấn công truy cập và thực hiện các hành vi trái phép - Ảnh hưởng: ProjectSend - Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế	https://nvd.nist.gov/vuln/detail/CVE-2024-11680
4	CVE-2024-0012	- Điểm CVSS: 9.8 (Nghiêm trọng) - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực hiện tấn công leo thang đặc quyền - 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-2024-0012
5	CVE-2024-9474	- Điểm CVSS: 7.2 (Cao) - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực hiện tấn công leo thang đặc quyền - 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-2024-9474
6	CVE-2024-44308	- Điểm CVSS: 8.8 (Cao) - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã từ xa - Ảnh hưởng: Safari, iOS, iPadOS, macOS, visionOS của Apple - Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế	https://nvd.nist.gov/vuln/detail/CVE-2024-44308
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	https://nvd.nist.gov/vuln/detail/CVE-2024-47575

		- Ảnh hưởng: FortiManager - Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế	
8	CVE-2024-44309	- Điểm CVSS: 6.1 (Trung bình) - Mô tả: Lỗ hổng cho phép đối tượng tấn công truy cập và thực hiện các hành vi trái phép - Ảnh hưởng: Safari, iOS, iPadOS, macOS, visionOS của Apple - Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế	https://nvd.nist.gov/vuln/detail/CVE-2024-44309
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 Collaboration (ZCS) - 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-2024-9264	- Điểm CVSS: 8.8 (Cao) - Mô tả: Lỗ hổng cho phép đối tượng tấn công khai thác lỗi Command Injection, truy cập và thực hiện các hành vi trái phép. - Ảnh hưởng: Grafana - Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế	https://nvd.nist.gov/vuln/detail/CVE-2024-9264
11	CVE-2023-32428	- 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: macOS, tvOS, iOS, iPadOS, watchOS của Apple - Lỗ hổng chưa có mã khai thác và đang bị khai thác trong thực tế	https://nvd.nist.gov/vuln/detail/CVE-2023-32428
12	CVE-2024-47533	- 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.	https://nvd.nist.gov/vuln/detail/CVE-2024-47533

		- Ảnh hưởng: Cobbler trên Linux - Lỗ hổng chưa có mã khai thác và đang bị khai thác trong thực tế	

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 2448/CATTT-NCSC về việc Cảnh báo chiến dịch tấn công có chủ đích của nhóm APT Earth Estriesr phát hành ngày 22/11/2024.

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 **11/2024**, Trung tâm NCSC phát hiện **17 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:
- 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;

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

- Các phòng: ATHTTT, TT&HTQT;
- Trung tâm VNCERT/CC;
- Lưu: VT, NCSC.LTQ.

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	shop[.]shopamzselling[.]com	Website giả mạo sàn TMĐT Amazon
2	https://sellings-global[.]com/shop	Website giả mạo sàn TMĐT Amazon
3	https://sellings-global[.]com/fedex	Website giả mạo sàn TMĐT Amazon
4	https://amazoui[.]top/	Website giả mạo sàn TMĐT Amazon
5	https://amazoni1[.]com/	Website giả mạo sàn TMĐT Amazon
6	https://www[.]applecenter[.]info[.]vn/	Website giả mạo sàn TMĐT Apple
7	https://apps[.]apple[.]com/VNapp/id6738024808	Website giả mạo sàn TMĐT Apple
8	clash-flow-loan[.]com	Website giả mạo Bộ Công an
9	https://dichvucongbca[.]com/	Website giả mạo Bộ Công an
10	dichvucong[.]thongtincancuoc[.]org	Website giả mạo Bộ Công An
11	giaohangtietkiem-cskh[.]com	Website giả mạo Công ty cổ phần giao hàng tiết kiệm
12	giaohangtietkiem247[.]com[.]vn	Website giả mạo Công ty cổ phần giao hàng tiết kiệm
13	https://nhanvienhanghoa[.]com/index/user/index[.]html	Website giả mạo Công ty cổ phần giao hàng tiết kiệm

14	https://chat[.]dichvutonghop[.]vip/index/index/home?visiter_id=&visiter_name=&avatar=&business_id=1&groupid=8&special=32	Website giả mạo Công ty cổ phần giao hàng tiết kiệm
15	https://giaohangtietkiem24[.]com/	Website giả mạo Công ty cổ phần giao hàng tiết kiệm
16	Giaohangtietkiemm[.]net	Website giả mạo Công ty cổ phần giao hàng tiết kiệm
17	https://www[.]ihomeficvn[.]com	Website giả mạo Công ty Tài chính TNHH MTV Home Credit Việt Nam
18	https://aeoonmallstore[.]com/	Website giả mạo Công ty TNHH Aeon Việt Nam
19	https://aeoonmallstore[.]com/my	Website giả mạo Công ty TNHH Aeon Việt Nam
20	dkvn[.]zvogo[.]com	Website giả mạo Cục Đăng kiểm Việt Nam
21	https://dkvn[.]zvogo[.]com/	Website giả mạo Cục Đăng kiểm Việt Nam
22	vn-chinhphu[.]com	Website giả mạo Dịch vụ công Quốc Gia
23	dichvucong[.]wrgov[.]com	Website giả mạo Dịch vụ công Quốc Gia
24	dienmayxanh-services[.]com	Website giả mạo Điện máy xanh
25	https://ebayve[.]com	Website giả mạo sàn TMĐT Ebay
26	lazada[.]ac	Website giả mạo sàn TMĐT Lazada
27	lazada2024[.]online	Website giả mạo sàn TMĐT Lazada
28	bidvnanghanguutien[.]duy2[.]name[.]vn	Website giả mạo Ngân Hàng TMCP Đầu tư và Phát triển Việt Nam

29	hdbank[.]uudaikhachhang-trungtamcapnhatthe-thang11[.]com[.]vn	Website giả mạo Ngân hàng TMCP Phát triển Thành phố Hồ Chí Minh
30	hdbank[.]chamsockhachhang-hotro247-capnhatuudai-thang11[.]com[.]vn	Website giả mạo Ngân hàng TMCP Phát triển Thành phố Hồ Chí Minh
31	hdbank[.]uudaidacbiet-khuyenmaikhachhang-thang11[.]com[.]vn	Website giả mạo Ngân hàng TMCP Phát triển Thành phố Hồ Chí Minh
32	https://ocbcccreonline[.]com/	Website giả mạo Ngân hàng TMCP Phương Đông
33	https://vimoney[.]credit	Website giả mạo Ngân hàng TMCP Quân đội
34	Ungdung6buoc[.]com	Website giả mạo Ngân hàng TMCP Quân đội
35	https://mmmbonline[.]com	Website giả mạo Ngân hàng TMCP Quân đội
36	https://www[.]iplus-fianc24h[.]online	Website giả mạo Ngân hàng TMCP Quân đội
37	khachhangcnvib[.]com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
38	vaythechapvib[.]com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
39	vib[.]khach-hang-nang-han-muc-ca-nhan[.]com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
40	vib[.]chamsockhachhang-capnhatthethang11[.]com[.]vn	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
41	doitac[.]shb-bank[.]com	Website giả mạo Ngân hàng TMCP Sài Gòn – Hà Nội
42	vpbank[.]cskhtructuyen-uudaithang10[.]com[.]vn	Website giả mạo Ngân hàng TMCP Việt Nam Thịnh Vượng
43	https://vpbank[.]uudaikhachhang-uudaithe-thang11[.]com[.]vn/	Website giả mạo Ngân hàng TMCP Việt Nam Thịnh Vượng

44	vpbank[.]chamsockhachhang-hotro247-trungtamcapnhatthe-thang11[.]com[.]vn	Website giả mạo Ngân hàng TMCP Việt Nam Thịnh Vượng
45	vpbank[.]khuyenmaidacbiet-uudaikhachhang-thang11[.]com[.]vn	Website giả mạo Ngân hàng TMCP Việt Nam Thịnh Vượng
46	https://vpbank[.]hotrokhachhang-khuyenmaithethang11[.]com[.]vn/	Website giả mạo Ngân hàng TMCP Việt Nam Thịnh Vượng
47	https://shinhan[.]hotrokhachhang-uudaithemoi-thang11[.]com[.]vn/	Website giả mạo Ngân hàng TNHH MTV Shinhan Việt Nam
48	https://shinhan[.]hotrokhachhang-uudaithemoi-thang11[.]com[.]vn	Website giả mạo Ngân hàng TNHH MTV Shinhan Việt Nam
49	https://shinhan[.]chamsockhachhang-hotro247-capnhatthe-thang11[.]com[.]vn	Website giả mạo Ngân hàng TNHH MTV Shinhan Việt Nam
50	www[.]sp7588p[.]com	Website giả mạo sàn TMĐT Shopee
51	https://sp56188p[.]com/my	Website giả mạo sàn TMĐT Shopee
52	https://nzu62352s[.]com/order	Website giả mạo sàn TMĐT Shopee
53	https://sp5583p[.]com/my	Website giả mạo sàn TMĐT Shopee
54	https://evnsp[.]com/	Website giả mạo Tập đoàn Điện lực Việt Nam (EVN)
55	https://www[.]evnsspc[.]com/	Website giả mạo Tập đoàn Điện lực Việt Nam (EVN)
56	www[.]evnspc[.]com	Website giả mạo Tập đoàn Điện lực Việt Nam (EVN)
57	https://evnspccskh[.]com	Website giả mạo Tập đoàn Điện lực Việt Nam (EVN)
58	evnspccskh[.]com	Website giả mạo Tập đoàn Điện lực Việt Nam (EVN)
59	tikione[.]vip	Website giả mạo sàn TMĐT Tiki

60	tikifreeship[.]xyz	Website giả mạo sàn TMĐT Tiki
61	https://www[.]tikifreeship[.]cc	Website giả mạo sàn TMĐT Tiki
62	https://tiktok-svip11[.]com/r?code=YFVEZA	Website giả mạo TikTok
63	https://nappxutiktok[.]com/?gad_source=1&gclid=Cj0KCQiA57G5BhDUARIsACgCYnwlJ3b-Bz8QcfBB4TipigL3qZOu58RxALHVNJqDNA82kM2MwgBOM30aApa0EALw_wcB#	Website giả mạo TikTok
64	https://af[.]tiktok25881[.]shop/	Website giả mạo TikTok
65	Evaluatetravels[.]com	Website giả mạo Traveloka
66	https://evaluatetravels[.]com/login	Website giả mạo Traveloka
67	https://evaluatetravels[.]com/recharge	Website giả mạo Traveloka
68	https://evaluatetravels[.]com/my/history-recharge-withdraw	Website giả mạo Traveloka
69	https://chinhphu[.]khaibaoshkdt[.]com/	Website giả mạo Văn phòng Chính phủ
70	vietnamtctgooc[.]com	Website giả mạo Văn phòng Chính phủ
71	chinh-phu[.]cc	Website giả mạo Văn phòng Chính phủ
72	https://chinhphu-vn[.]com/	Website giả mạo Văn phòng Chính phủ
73	vnairlines[.]net	Website giả mạo Vietnam Airlines
74	https://phucloixahoi[.]quandoiviettel[.]com/	Website giả mạo Viettel

75	https://viettel-post[.]cfd/vn/	Website giả mạo ViettelPost
76	https://nhantienquoctej13[.]vercel[.]app/dichvunhantien	Website giả mạo Western Union
77	https://zloweb[.]me/	Website giả mạo Zalo

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	14343	https://nvd.nist.gov/vuln/detail/ CVE-2022-26809
2	CVE-2023-21716	6467	https://nvd.nist.gov/vuln/detail/ CVE-2023-21716
3	CVE-2024-48618	5143	https://nvd.nist.gov/vuln/detail/ CVE-2024-48618
4	CVE-2024-49046	4722	https://nvd.nist.gov/vuln/detail/ CVE-2024-49046
5	CVE-2023-40477	2267	https://nvd.nist.gov/vuln/detail/ CVE-2024-40477
6	CVE-2024-10827	1531	https://nvd.nist.gov/vuln/detail/ CVE-2024-10827
7	CVE-2024-49039	1521	https://nvd.nist.gov/vuln/detail/ CVE-2021-49039
8	CVE-2021-40444	1297	https://nvd.nist.gov/vuln/detail/ CVE-2024-40444
9	CVE-2024-10488	1277	https://nvd.nist.gov/vuln/detail/ CVE-2024-10488
10	CVE-2023-38831	1197	https://nvd.nist.gov/vuln/detail/ CVE-2021-38831

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	103.96.128[.]44	Nhóm APT Evasive Panda
2	AD6C84859D413D627AC589AEDF9891707E179D6C	
3	348730018E0A5554F0F05E47BBA43DC0F55795AC	
4	C058F9FE91293040C8B0908D3DAFC80F89D2E38B	
5	B3556D1052BF5432D39A6068CCF00D8C318AF146	
6	8EAA213AE4D482938C5A7EC523C83D2C2E1E8C0E	
7	C70C3750AC6B9D7B033ADDEF838EF1CC28C262F3	
8	3DD958CA6EB7E8F0A0612D295453A3A10C08F5FE	
9	9B6A473820A72111C1A38735992B55C413D941EE	
10	4A5BCDAAC0BC315EDD00BB1FCCD1322737BCBEEB	
11	84F6B9F13CDCD8D9D15D5820536BC878CD89B3C8	
12	A1CA41FDB61F03659168050DE3E208F0940F37D8	
13	812124B84C5EA455F7147D94EC38D24BDF159F84	
14	547BD65EEE05D744E075C5E12FB973A74D42438F	
15	621E2B50A979D77BA3F271FAB94326CCCBC009B4	
16	67028AEB095189FDF18B2D7B775B62366EF224A9	

17	93C1C8AD2AF64D0E4C132F067D369ECBEBAE00B7	
18	SafeShift390[.]onmicrosoft[.]com	Chiến dịch tấn công “VEILDrive”
19	40.90.196[.]221	
20	38.180.136[.]85	
21	GreenGuard036[.]onmicrosoft[.]com	
22	40.90.196[.]228	
23	213.87.86[.]192	
24	hxxps[://]tvdseo[.]com/file/synaptics[.]zip	Chiến dịch tấn công sử dụng mã độc “PXA Stealer” thực hiện bởi nhóm tấn công mạng gốc Việt.
25	hxxps[://]tvdseo[.]com/file/Adonis/AdFnis_Bot	
26	hxxps[://]tvdseo[.]com/file/Adonis/Adonis_XW_ENC	
27	hxxps[://]tvdseo[.]com/file/STC/STC_XW_ENC	
28	hxxps[://]tvdseo[.]com/file/STC/STC_OTO	
29	hxxps[://]tvdseo[.]com/file/STC/STC_BOT	
30	hxxps[://]tvdseo[.]com/file/STC/STC_PUP	
31	hxxps[://]tvdseo[.]com/file/STC/STC_PURE_ENC	
32	tvdseo[.]com	
33	hxxps[://]tvdseo[.]com/file/PXA/PXA_PURE_ENC	
34	hxxps[://]tvdseo[.]com/file/PXA/PXA_PURE_ENC	
35	hxxps[://]tvdseo[.]com/file/Adonis/Adonis_Bot0	

36	hxxps[://]tvdseo[.]com/file/STC/STC_PURE[.]b64	
37	hxxps[://]tvdseo[.]com/file/PXA/Cookie_Ext[.]zip	
38	hxxps[://]tvdseo[.]com/file/PXA/PXA_BOT	
39	hxxps[://]tvdseo[.]com/file/PXA/PXA_BOT	
40	hxxps[://]tvdseo[.]com/file/Adonis/Adonis_Bot	
41	hxxps[://]tvdseo[.]com/file/STC/Cookie_Ext[.]zip	
42	149[.]248[.]14[.]53	Nhóm APT “Gelsemium”
43	4vw37z[.]cn	
44	domain[.]dns04[.]com	
45	microsoftservice[.]dns1[.]us	
46	sitesafecdn[.]hopto[.]org	
47	www[.]sitesafecdn[.]dynamic-dns[.]net	
48	210[.]209[.]72[.]180	
49	acro[.]ns1[.]name	
50	info[.]96html[.]com	
51	pctftp[.]otzo[.]com	
52	traveltime[.]hopto[.]org	
53	www[.]travel[.]dns04[.]com	