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: 13 /BC-CATTT

Hà Nội, ngày 09 tháng 08 năm 2024

BÁO CÁO AN TOÀN THÔNG TIN MẠNG VIỆT NAM
(Tháng 7/2024)

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 **7/2024**, 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 **7/2024**, 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 25/8/2024.**

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

Văn bản số 1310/CATTT-NCSC về việc lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 07/2024 phát hành ngày 12/07/2024.

Trung tâm NCSC đã phát hành các tin cảnh báo hàng tuần trên https://khonggianmang.vn/ về các vấn đề an toàn thông tin trên không gian mạng; ghi nhận, thống kê số liệu về tình trạng an toàn thông tin tại Việt Nam trong tháng vừa qua.

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 **7/2024** 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 **7/2024** 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 **82/88 đơn vị** có kết nối thường xuyên. Trong các đơn vị kết nối thường xuyên có **82/82 đơn vị** chia sẻ về hệ điều hành các máy **(tổng số máy là 274.557)**.

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

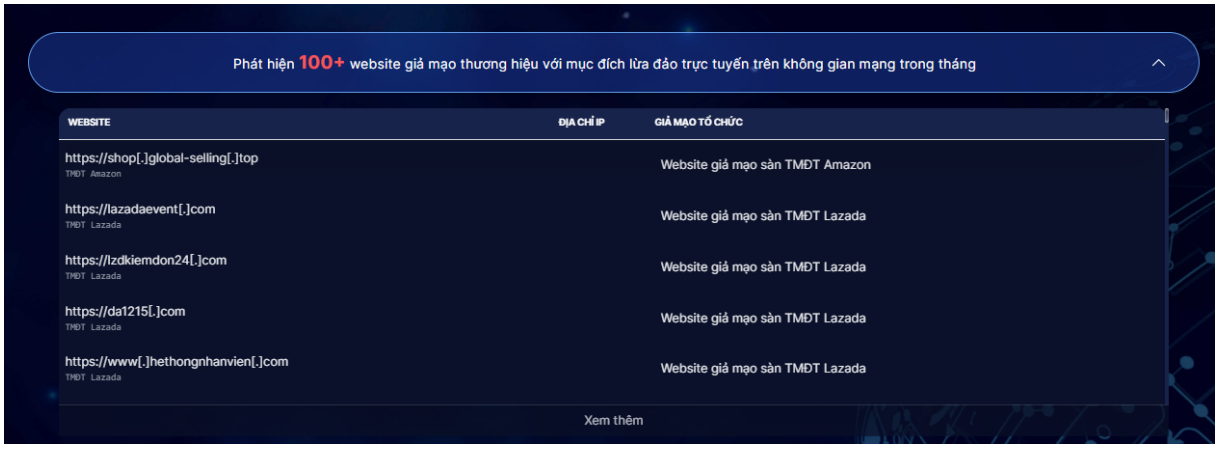
3. Phát hiện và ngăn chặn lừa đảo trên không gian mạng

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 **125.059 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 **7/2024**, hệ thống của NCSC đã phát hiện **125 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 **36.497** 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 **7/2024**, 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 7/2024:

TT	Mã điểm yếu/lỗ hổng	Mô tả	Ghi chú
1	CVE-2024-6387	- Điểm CVSS: 8.1 (Cao) - Mô tả: Lỗ hổng cho phép đối tượng tấn công truy cập và thực thi các hành vi trái phép. - Ảnh hưởng: OpenSSH. - Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.	https://nvd.nist.gov/vuln/detail/CVE-2024-6387
2	CVE-2024-6327	- Điểm CVSS: 9.8 (Nghiêm trọng) - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Progress Telerik Report Server - Lỗ hổng đang bị khai thác trong thực tế.	https://nvd.nist.gov/vuln/detail/CVE-2024-6327
3	CVE-2023-45249	- 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-2023-45249

		- Ảnh hưởng: Acronis Cyber Infrastructure - Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.	
4	CVE-2024-36401	- Điểm CVSS: 9.8 (Nghiêm trọng) - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: GeoServer - Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.	https://nvd.nist.gov/vuln/detail/CVE-2024-36401
5	CVE-2024-23692	- Điểm CVSS: 9.8 (Nghiêm trọng) - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Rejetto HTTP File Server - Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.	https://nvd.nist.gov/vuln/detail/CVE-2024-23692
6	CVE-2024-38112	- Điểm CVSS: 7.5 (Cao) - Mô tả: Lỗ hổng cho phép đối tượng tấn công truy cập và thực thi các hành vi trái phép. - Ảnh hưởng: Windows 10, Windows 11, Windows Server 2008, Windows Server 2012, Windows Server 2016, Windows Server 2019, Windows Server 2022. - Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.	https://nvd.nist.gov/vuln/detail/CVE-2024-38112
7	CVE-2024-37085	- Điểm CVSS: 6.8 (Cao) - Mô tả: Lỗ hổng cho phép đối tượng tấn công truy cập và thực thi các hành vi trái phép. - Ảnh hưởng: VMware ESXi - Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.	https://nvd.nist.gov/vuln/detail/CVE-2024-37085
8	CVE-2024-36991	- Điểm CVSS: 7.5 (Cao)	https://nvd.nist.gov/vuln/detail/CVE-2024-36991

		- Mô tả: Lỗ hổng cho phép đối tượng tấn công truy cập và thực thi các hành vi trái phép. - Ảnh hưởng: Splunk Enterprise trên Windows. - Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.	
9	CVE-2006-5051	- Điểm CVSS: 8.1 (Cao) - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ, thực thi mã từ xa. - Ảnh hưởng: OpenSSH. - Lỗ hổng đang bị khai thác trong thực tế.	https://nvd.nist.gov/vuln/detail/CVE-2006-5051
10	CVE-2024-20419	- Điểm CVSS: 10.0 (Nghiêm trọng) - Mô tả: Lỗ hổng cho phép đối tượng tấn công truy cập và thực thi các hành vi trái phép. - Ảnh hưởng: Cisco Smart Software Manager On-Prem - Lỗ hổng đang bị khai thác trong thực tế.	https://nvd.nist.gov/vuln/detail/CVE-2024-20419
11	CVE-2024-20401	- Điểm CVSS: 9.8 (Nghiêm trọng) - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ, thực thi mã từ xa, truy cập và thực thi các hành vi trái phép - Ảnh hưởng: Cisco Secure Email Gateway - Lỗ hổng đang bị khai thác trong thực tế.	https://nvd.nist.gov/vuln/detail/CVE-2024-20401
12	CVE-2024-21412	- Điểm CVSS: 8.1 (Cao) - Mô tả: Lỗ hổng cho phép đối tượng tấn công truy cập và thực thi các hành vi trái phép. - Ảnh hưởng: Windows 10, Windows 11, Windows 2019, Windows 2022. - Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.	https://nvd.nist.gov/vuln/detail/CVE-2024-21412

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 1310/CATTT-NCSC ngày 12/7/2024 về việc lỗ hổng an toàn thông tin ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 07/2024.

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 **7/2024**, Trung tâm NCSC phát hiện **19 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;
- PCT Trần Đăng Khoa;
- Các phòng: ATHTTT, TT&HTQT;
- Trung tâm VNCERT/CC;
- Lưu: VT, NCSC.LTQ.

CỤC TRƯỞNG

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

Lê Văn Tuấn

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	https://baohiemxahoi[.]vnagov[.]com	Website giả mạo Bảo hiểm Xã hội Việt Nam
6	https://vssid[.]govnn[.]cc/	Website giả mạo Bảo hiểm Xã hội Việt Nam
7	https://mojgov[.]weebly[.]com	Website giả mạo Bộ Tư pháp
8	https://icchanoi[.]net/	Website giả mạo Công ty Cổ phần Đầu tư Quốc tế ICC Hà Nội
9	nappthe[.]vn	Website giả mạo Công Ty Cổ Phần Giải Trí Và Thể Thao Điện Tử Việt Nam
10	https://giiao[.]hangtietkiem[.]com	Website giả mạo Công ty cổ phần giao hàng tiết kiệm
11	https://vgiao[.]hangtietkiem[.]com/	Website giả mạo Công ty cổ phần giao hàng tiết kiệm
12	bachhoaxanhh[.]com	Website giả mạo Công ty cổ phần Thương mại Bách Hóa Xanh

13	https://homecredit[.]hethongvaynhanh247[.]com/	Website giả mạo Công ty Tài chính TNHH MTV Home Credit Việt Nam
14	https://nqsncoau[.]buzz/	Website giả mạo Cty tài chính tnhh ngân hàng việt nam thịnh vượng smbc
15	https://dienmayxanhctv24[.]com	Website giả mạo Điện máy xanh
16	https://thisinhthanhlich2024[.]com	Website giả mạo Facebook
17	https://binhchoncuocthivetranhsinhvien2024[.]weebly[.]com	Website giả mạo Facebook
18	https://mfacebook-com[.]vn/	Website giả mạo Facebook
19	https://bethivetranh2024[.]weebly[.]com	Website giả mạo Facebook
20	https://events[.]pubg-vnggame[.]com	Website giả mạo Facebook
21	https://duyetdonlazada[.]com	Website giả mạo sàn TMĐT Lazada
22	https://da8975[.]com	Website giả mạo sàn TMĐT Lazada
23	https://la5959[.]com	Website giả mạo sàn TMĐT Lazada
24	https://www[.]iazada[.]com/	Website giả mạo sàn TMĐT Lazada
25	https://www[.]hethongnhanvien[.]com	Website giả mạo sàn TMĐT Lazada
26	https://da1215[.]com	Website giả mạo sàn TMĐT Lazada
27	https://lazadaevent[.]com/	Website giả mạo sàn TMĐT Lazada
28	https://lzdkiemdon24[.]com	Website giả mạo sàn TMĐT Lazada

29	https://www[.]momoshopvip[.]com	Website giả mạo MoMo
30	https://www[.]baovietcom[.]vip/	Website giả mạo Ngân hàng TMCP Bảo Việt
31	https://www[.]baovietn[.]vip	Website giả mạo Ngân hàng TMCP Bảo Việt
32	moneytracking137[.]com	Website giả mạo Ngân Hàng TMCP Công Thương Việt Nam
33	https://vietinbankamc[.]vn	Website giả mạo Ngân Hàng TMCP Công Thương Việt Nam
34	https://tcbcanhan[.]com	Website giả mạo Ngân hàng TMCP Kỹ Thương Việt Nam
35	https://khtechcanhan[.]com/	Website giả mạo Ngân hàng TMCP Kỹ Thương Việt Nam
36	https://vietcombank-career[.]com	Website giả mạo Ngân Hàng TMCP Ngoại thương Việt Nam
37	cskhcanhanhd[.]com	Website giả mạo Ngân hàng TMCP Phát triển Thành phố Hồ Chí Minh
38	hdbank[.]tructuyen-uudai-thekhachhang[.]com	Website giả mạo Ngân hàng TMCP Phát triển Thành phố Hồ Chí Minh
39	https://vnmcrd2s[.]online	Website giả mạo Ngân hàng TMCP Quân đội
40	https://mbdk99[.]com	Website giả mạo Ngân hàng TMCP Quân đội
41	https://www[.]dangnhaphoso[.]com	Website giả mạo Ngân hàng TMCP Quân đội
42	https://tcvnhomefic[.]com	Website giả mạo Ngân hàng TMCP Quân đội
43	https://mcqdvn[.]com	Website giả mạo Ngân hàng TMCP Quân đội
44	https://mmb-online[.]com	Website giả mạo Ngân hàng TMCP Quân đội

45	vib-care[.]com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
46	http://dich-vu-the-sat-vib[.]com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
47	https://vib[.]chamsockhachhang-uudai-tructuyenthe[.]com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
48	http://dich-vu-the-elite-vib[.]com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
49	https://vib[.]chamsockhachhang-tructuyenuudaithe[.]online	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
50	dich-vu-the-vvip-vib[.]com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
51	visa-vibbank[.]com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
52	https://dich-vu-the-svip-vib[.]com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
53	https://nang-cap-ocare-vib[.]com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
54	vib-nangcap[.]com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
55	main-card-vib[.]com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
56	vib-up-the[.]shop	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
57	vib-cardnew[.]shop	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
58	vib-nang-the[.]com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
59	nang-cap-the-vcare-vib[.]com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
60	nang-cap-qcare-vib[.]com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
61	vib-solution[.]shop	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam

62	http://vib[.]uudaikhachhang-tructuyen[.]com[.]vn	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
63	http://ib-miles-card[.]shop	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
64	http://vib-gold-card[.]shop	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
65	http://nang-hang-the-vip2-vib[.]com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
66	http://nang-hang-the-vip3-vib[.]com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
67	http://vib-khcn[.]shop/	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
68	vib-town[.]com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
69	https://tpbank[.]chamsockhachhang-uudaithe-thang6[.]com	Website giả mạo Ngân hàng TMCP Tiên Phong
70	www[.]vpbank[.]chamsockhachhang-uudaithecanhan-tructuyen[.]online	Website giả mạo Ngân hàng TMCP Việt Nam Thịnh Vượng
71	vpbank[.]uudai-tructuyen-chamsockhachhang-the[.]com[.]vn	Website giả mạo Ngân hàng TMCP Việt Nam Thịnh Vượng
72	https://www[.]vpbank[.]chamsockhachhang-uudai-the-truc-tuyen[.]online	Website giả mạo Ngân hàng TMCP Việt Nam Thịnh Vượng
73	https://www[.]tinchapshinhan[.]online	Website giả mạo Ngân hàng TNHH MTV Shinhan Việt Nam
74	https://centralmarketing[.]online/	Website giả mạo Ngân hàng Worldbank Việt Nam
75	https://lapdatinternet[.]net/	Website giả mạo SCTV
76	https://sendotv[.]com	Website giả mạo sàn TMĐT Sendo
77	https://sp75193p[.]com	Website giả mạo sàn TMĐT Shopee
78	https://sp1663p[.]com	Shopee

79	https://www[.]vn999mall[.]vip	Website giả mạo sàn TMĐT Shopee
80	https://sp1776p[.]com	Website giả mạo sàn TMĐT Shopee
81	sp7335p[.]com	Website giả mạo sàn TMĐT Shopee
82	https://vnc63661s[.]com	Website giả mạo sàn TMĐT Shopee
83	https://www[.]seleeashopee[.]com	Website giả mạo sàn TMĐT Shopee
84	https://vnc75635s[.]com	Website giả mạo sàn TMĐT Shopee
85	https://vnc69977s[.]com	Website giả mạo sàn TMĐT Shopee
86	https://www[.]shopeesop[.]com	Website giả mạo sàn TMĐT Shopee
87	https://nze98582s[.]com/	Website giả mạo sàn TMĐT Shopee
88	https://odz68254s[.]com	Website giả mạo sàn TMĐT Shopee
89	https://soppe86[.]life	Website giả mạo sàn TMĐT Shopee
90	https://www[.]sp5118p[.]com	Website giả mạo sàn TMĐT Shopee
91	https://www[.]govgdt[.]top	Website giả mạo Tập đoàn Điện lực Việt Nam (EVN)
92	https://www[.]thanhtrapcrt[.]online	Website giả mạo Thanh tra Chính phủ
93	https://fajiafu50[.]com	Website giả mạo sàn TMĐT Tiki
94	https://vntiki1[.]com	Website giả mạo sàn TMĐT Tiki
95	https://tdkt00[.]com	Website giả mạo sàn TMĐT Tiki

96	https://zla653[.]top	Website giả mạo sàn TMĐT Tiki
97	https://tdkt04[.]com	Website giả mạo sàn TMĐT Tiki
98	https://s2rjtiki[.]com	Website giả mạo sàn TMĐT Tiki
99	https://k2rjtiki[.]com	Website giả mạo sàn TMĐT Tiki
100	https://sh2tiki[.]com	Website giả mạo sàn TMĐT Tiki
101	https://tdkt06[.]com	Website giả mạo sàn TMĐT Tiki
102	https://fajiafu30[.]com/	Website giả mạo sàn TMĐT Tiki
103	https://tdkt07[.]com	Website giả mạo sàn TMĐT Tiki
104	https://tikijaj2[.]com	Website giả mạo sàn TMĐT Tiki
105	https://tikt88[.]com	Website giả mạo sàn TMĐT Tiki
106	https://businesseventskp[.]top	Website giả mạo sàn TMĐT Tiki
107	https://www[.]tikifreeship[.]vip/	Website giả mạo sàn TMĐT Tiki
108	https://tdke00[.]com/	Website giả mạo sàn TMĐT Tiki
109	https://www[.]vntiki[.]vip	Website giả mạo sàn TMĐT Tiki
110	https://tdke02[.]com	Website giả mạo sàn TMĐT Tiki
111	https://nhanvientiki[.]org	Website giả mạo sàn TMĐT Tiki
112	https://muasamtiki[.]com	Website giả mạo sàn TMĐT Tiki

113	https://tracuutthvt[.]com	Website giả mạo Tổng cục Thuế
114	chinhphu[.]cc	Website giả mạo Văn phòng Chính phủ
115	https://chinhphu[.]dancuquocgia[.]org	Website giả mạo Văn phòng Chính phủ
116	https://viettlot135p[.]com	Website giả mạo Vietlott
117	quandoi-viettel[.]com	Website giả mạo Viettel
118	Giaodichquoctes[.]com	Website giả mạo Western Union
119	https://giaodichquoctes[.]vercel[.]app	Website giả mạo Western Union
120	https://giaodichquoctes[.]com	Website giả mạo Western Union
121	https://nhantienquoctev3[.]vercel[.]app/	Website giả mạo Western Union
122	https://chuyentienquoctenhanh[.]vercel[.]app/	Website giả mạo Western Union
123	chuyentienquocte1313[.]vercel[.]app	Website giả mạo Western Union
124	giaodichdaquocgia[.]us	Website giả mạo Western Union
125	https://xacnhanthutuchoantra[.]us/	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	15834	https://nvd.nist.gov/vuln/detail/ CVE-2022-26809
2	CVE-2023-21716	6752	https://nvd.nist.gov/vuln/detail/ CVE-2023-21716
3	CVE-2023-29341	1408	https://nvd.nist.gov/vuln/detail/ CVE-2023-29341
4	CVE-2021-40444	995	https://nvd.nist.gov/vuln/detail/ CVE-2021-40444
5	CVE-2024-30093	958	https://nvd.nist.gov/vuln/detail/ CVE-2024-30093
6	CVE-2024-37985	807	https://nvd.nist.gov/vuln/detail/ CVE-2024-37985
7	CVE-2021-28310	786	https://nvd.nist.gov/vuln/detail/ CVE-2021-28310
8	CVE-2023-36732	725	https://nvd.nist.gov/vuln/detail/ CVE-2023-36732
9	CVE-2024-35265	579	https://nvd.nist.gov/vuln/detail/ CVE-2024-35265
10	CVE-2020-1097	565	https://nvd.nist.gov/vuln/detail/ CVE-2020-1097

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	bba3b15bad6b5a80ab9fa9a49b643658	Nhóm APT Kimsuky
2	38e27983c757374d9bae36a2e2520e8e	
3	hxxp://sdfa.liveblog365[.]com/ares/hades.txt	
4	hxxp://sdfa.liveblog365[.]com/ares/babyhades.txt	
5	hxxp://ney.r-e[.]kr/mar/tys.txt	
6	hxxp://ney.r-e[.]kr/mar/tys.php	
7	hxxps://webman.w3school.cloudns[.]nz	
8	hxxps://onewithshare.blogspot[.]com/2023/04/10.html	
9	hxxps://raw.githubusercontent[.]com/HelperDav/Web/main/update.xml	
10	hxxps://github[.]com/cmastern	
11	0d068b6d0523f069d1ada59c12891c4a	Nhóm APT41
12	b3067f382d70705d4c8f6977a7d7bee4	
13	d72f202c1d684c9a19f075290a60920f	
14	294cc02db5a122e3a1bc4f07997956da	
15	393065ef9754e3f39b24b2d1051eab61	
16	bcac2cbda36019776d7861f12d9b59c4	

17	f062183da590aba5e911d2392bc29181	
18	4141c4b827ff67c180096ff5f2cc1474	
19	bc85062de0f70afd44bb072b0b71a8cc	
20	72070b165d1f11bd4d009a81bf28a3e5	
21	f0953ed4a679b987a2da955788737602	
22	hxxps[://]fullgasesspa[.]cl/tet/download[.]php	Nhóm APT VoidBanshee
23	hxxp[://]cbmelipilla[.]cl/te/test1[.]html	
24	hxxps[://]cbmelipilla[.]cl/te/hhhh2[.]php	
25	hxxps[://]hostalaskapatagonia[.]com/tt/tedfd[.]te	
26	hxxps[://]hostalaskapatagonia[.]com/tt/become[.]txt	
27	hxxp[://]h[.]com:8000/test1[.]html	
28	185[.]172[.]128[.]95	
29	4bb191c6d3a234743ace703d7d518f8f	Nhóm APT Ghost Emperor
30	43f1c44fa14f9ce2c0ba9451de2f7d3dd1a208de	
31	95e3312de43c1da4cc3be8fa47ab9fa4	
32	a59cca28205eeb94c331010060f86ad2f3d41882	
33	d8ebfd26bed0155e7c4ec2ca429c871d	
34	bab2ae2788dee2c41065850b2877202e57369f37	
35	imap.dateupdata[.]com	
36	193.239.86[.]168	

37	45[.]66[.]217[.]106	Nhóm APT MirrorFace
38	45[.]77[.]12[.]212	
39	207[.]148[.]97[.]235	
40	64[.]176[.]214[.]51	
41	45[.]76[.]222[.]130	
42	207[.]148[.]90[.]45	
43	103[.]143[.]208[.]115	
44	103[.]143[.]209[.]36	
45	91[.]245[.]255[.]30	
46	89[.]233[.]109[.]69	
47	108[.]160[.]130[.]45	
48	95[.]85[.]91[.]15	
49	168[.]100[.]8[.]103	
50	45[.]77[.]183[.]161	
51	207[.]148[.]103[.]42	
52	103[.]143[.]208[.]29	
53	146[.]70[.]79[.]68	
54	91[.]245[.]255[.]79	
55	www[.]morrowadded[.]com	

56	www[.]lookpumrron[.]com	Nhóm APT MirrorFace
57	minggamevies[.]com	
58	2a12:a300:3600::31b5:2e02	
59	2400:8902::f03c:93ff:fe8a:5327	
60	93af6afb47f4c42bc0da3eedc6ecb9054134f4a47ef0add0d285404984011072	
61	43349c97b59d8ba8e1147f911797220b1b7b87609fe4aaa7f1dbacc2c27b361d	
62	0d59734bdb0e6f4fe6a44312a2d55145e98b00f75a148394b2e4b86436c32f4c	
63	572f6b98cc133b2d0c8a4fd8ff9d14ae36cdaa119086a5d56079354e49d2a7ce	
64	5e7cd0461817b390cf05a7c874e017e9f44eef41e053da99b479a4dfa3a04512	
65	2001:19f0:7001:2ae2:5400:4ff:fe0a:5566	
66	2a12:a300:3700::5d9f:b451	
67	bcd34d436cbac235b56ee5b7273baed62bf385ee13721c7fdcfc00af9ed63997	
68	4f932d6e21fdd0072aba61203c7319693e490adbd9e93a49b0fe870d4d0aed71	
69	9590646b32fec3aafd6c648f69ca9857fb4be2adfabf3bcaf321c8cd25ba7b83	
70	7a7e7e0d817042e54129697947dfb423b607692f4457163b5c62ffea69a8108d	
71	b07c7dfb3617cd40edc1ab309a68489a3aa4aa1e8fd486d047c155c952dc509e	