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: 6 /BC-CATTT

Hà Nội, ngày 19 tháng 04 năm 2024

BÁO CÁO AN TOÀN THÔNG TIN MẠNG VIỆT NAM
(Tháng 3/2024)

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 **3/2024**, Cục An toàn thông tin (Bộ Thông tin và Truyền thông) phát hiện xu hướng tấn công mạng mã hóa tống tiền (ransomware) tăng cao. 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.

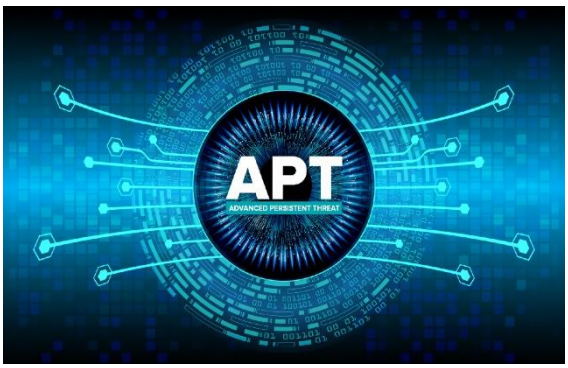
Cục An toàn thông tin đã phát hành Công văn số 476/CATTT-ATHTTT về việc tăng cường bảo đảm an toàn thông tin mạng đối với hệ thống thông tin ngày 30/03/2024, Công văn số 424/CATTT-NCSC về việc rà soát dấu hiệu của các chiến dịch tấn công có chủ đích (APT) ngày 22/3/2024.

Trong tháng **3/2024**, hệ thống giám sát, cảnh báo sớm rủi ro của Trung tâm NCSC 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, 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 đến các đơn vị.

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

Văn bản số 210/CATTT-NCSC về việc lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 02/2024 phát hành ngày 22/02/2024.

Văn bản số 424/CATTT-NCSC về việc rà soát dấu hiệu của các chiến dịch tấn công có chủ đích (APT) phát hành ngày 22/03/2024.



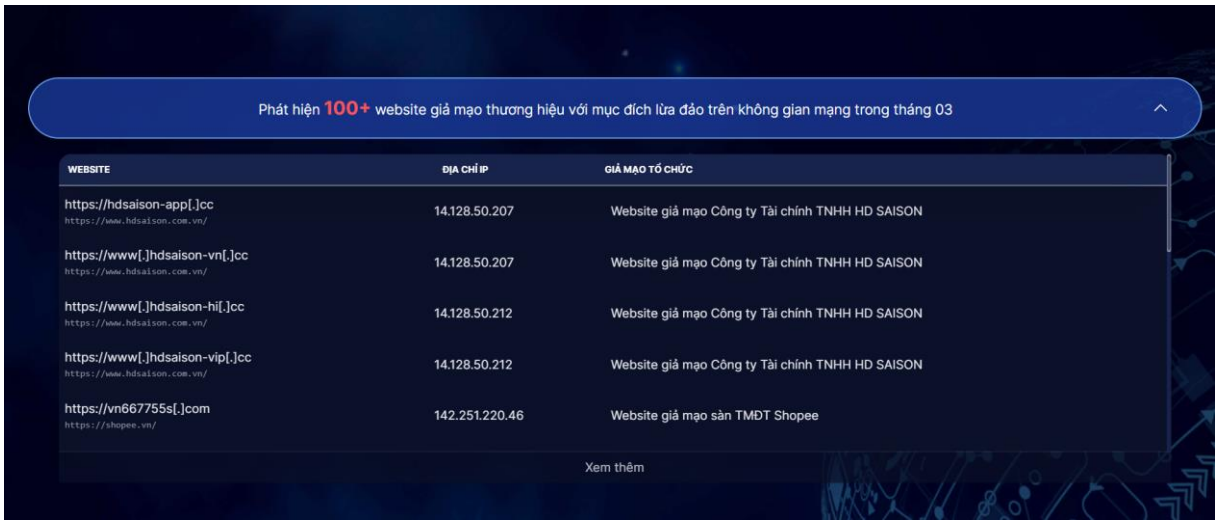
Văn bản số 476/CATTT-ATHTTT về việc tăng cường bảo đảm an toàn thông tin mạng đối với hệ thống thông tin phát hành ngày 30/03/2024.

2. 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 **124.579 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 **3/2024**, hệ thống của NCSC đã phát hiện hơn **100 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.*

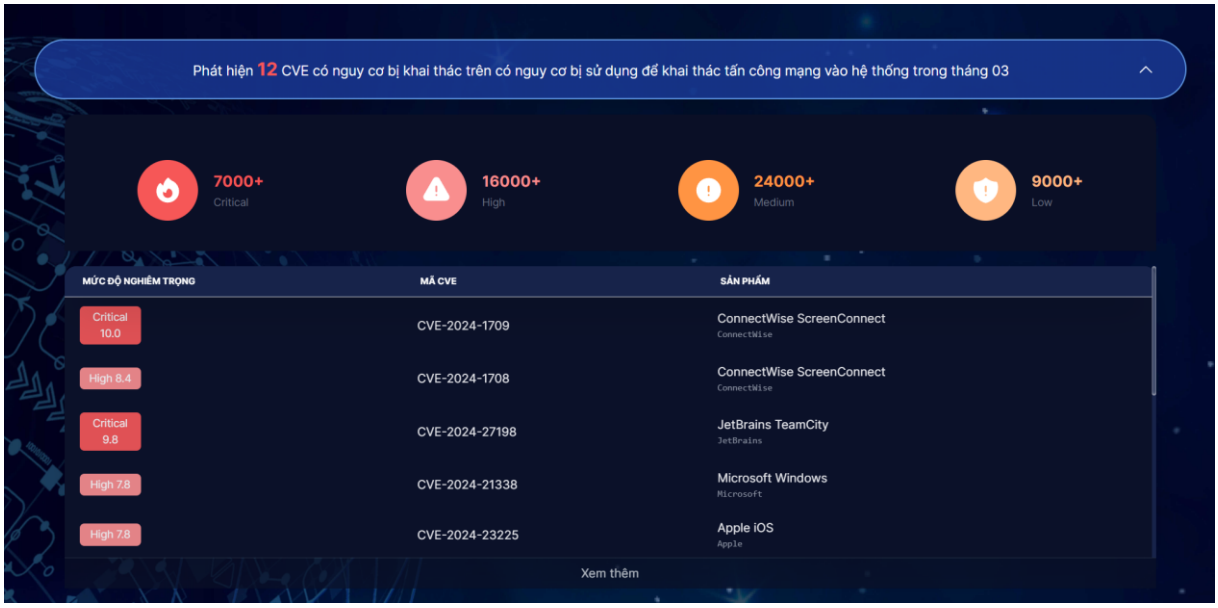
3. Phát hiện và cảnh báo sớm các lỗ hổng của các hệ thống thông tin trên không gian mạng

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 **88.990** 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 **3/2024**, 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 3/2024:

TT	Mã điểm yếu/lỗ hổng	Mô tả	Ghi chú
1	CVE-2024-1709	- Điểm CVSS: 10.0 (Nghiêm trọng) - Mô tả: Lỗ hổng cho phép đối tượng tấn công vượt qua bảo mật xác thực - Ảnh hưởng: ConnectWise ScreenConnect	https://nvd.nist.gov/vuln/detail/CVE-2024-1709
2	CVE-2024-1708	- Điểm CVSS: 8.4 (Nghiêm trọng) - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã từ xa, tác động trực tiếp tới dữ liệu và hệ thống. - Ảnh hưởng: ConnectWise ScreenConnect	https://nvd.nist.gov/vuln/detail/CVE-2024-1708

3	CVE-2024-27198	- Điểm CVSS: 9.8 (Nghiêm trọng) - Mô tả: Lỗ hổng cho phép đối tượng tấn công vượt qua bảo mật xác thực - Ảnh hưởng: JetBrains TeamCity. - Lỗ hổng hiện đang bị khai thác trong thực tế, và đã có mã khai thác.	https://nvd.nist.gov/vuln/detail/CVE-2024-27198
4	CVE-2024-21338	- 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 - Lỗ hổng đã có mã khai thác.	https://nvd.nist.gov/vuln/detail/CVE-2024-21338
5	CVE-2024-23225	- Điểm CVSS: 7.8 (Cao) - Mô tả: Lỗ hổng cho phép đối tượng tấn công gây ảnh hưởng tới bộ nhớ của thiết bị. - Ảnh hưởng: Apple iOS	https://nvd.nist.gov/vuln/detail/CVE-2024-23225
6	CVE-2024-27199	- Điểm CVSS: 7.3 (Cao) - Mô tả: Lỗ hổng cho phép đối tượng tấn công leo thang đặc quyền. - Ảnh hưởng: JetBrains TeamCity	https://nvd.nist.gov/vuln/detail/CVE-2024-27199
7	CVE-2024-20337	- Điểm CVSS: 8.2 (Nghiêm trọng) - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực hiện tấn công CRLF Injection - Ảnh hưởng: Cisco Secure Client - Lỗ hổng đã có mã khai thác.	https://nvd.nist.gov/vuln/detail/CVE-2024-20337
8	CVE-2024-23296	- Điểm CVSS: 7.8 (Cao) - Mô tả: Lỗ hổng cho phép đối tượng tấn công gây ảnh hưởng tới bộ nhớ của thiết bị. - Ảnh hưởng: Apple iOS	https://nvd.nist.gov/vuln/detail/CVE-2024-23296

9	CVE-2024-1071	- Điểm CVSS: 9.8 (Nghiêm trọng) - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực hiện tấn công SQL Injection. - Ảnh hưởng: WordPress - Lỗ hổng đã có mã khai thác.	https://nvd.nist.gov/vuln/detail/CVE-2024-1071
10	CVE-2024-23204	- 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 với dữ liệu của thiết bị. - Ảnh hưởng: Apple iOS	https://nvd.nist.gov/vuln/detail/CVE-2024-23204
11	CVE-2024-21887	- Điểm CVSS: 9.1 (Nghiêm trọng) - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực hiện tác vụ chèn mã, thực thi mã từ xa. - Ảnh hưởng: Ivanti Connect Secure, Ivanti Policy Secure	https://nvd.nist.gov/vuln/detail/CVE-2024-21887
12	CVE-2024-21893	- Điểm CVSS: 8.2 (Nghiêm trọng) - Mô tả: Lỗ hổng cho phép đối tượng tấn công khai thác lỗ hổng SSRF. - Ảnh hưởng: Ivanti Connect Secure, Ivanti Policy Secure	https://nvd.nist.gov/vuln/detail/CVE-2024-21893

4. 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 476/CATTT-ATHTTT ngày 30/3/2024 về việc tăng cường bảo đảm an toàn thông tin mạng đối với hệ thống thông tin.

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.*

5. 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 **3/2024**, Trung tâm NCSC phát hiện **09 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.

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 thông: điện thoại: 024.32091.616 hoặc số điện thoại trực đường dây nóng hỗ trợ giám sát, cảnh báo sớm 0961.405.333, thư điện tử: ais@mic.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 Cục: Viễn thông; Bưu điện Trung ương;
- Các Trung tâm: TTTT, VNNIC;
- Cục trưởng (để b/c);
- Các Phó Cục trưởng;
- Các phòng: ATHTTT, TT&HTQT;
- Trung tâm VNCERT/CC;
- Lưu: VT, NCSC.LTQ.

KT. CỤC TRƯỞNG
PHÓ CỤC TRƯỞNG

CỘNG HOÀ 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://abbankquick[.]com	Ngân hàng TMCP An Bình
2	https://apple[.]support-find-my-iphone[.]com/s113h	Website giả mạo Apple
3	https://www[.]taikhoanvps[.]com[.]vn	Website giả mạo Công ty chứng khoán VPS
4	https://motaikhoanchungkhoanvps[.]com	Website giả mạo Công ty chứng khoán VPS
5	https://hdsaison-com[.]cc	Website giả mạo Công ty Tài chính TNHH HD SAISON
6	https://hdsaison-app[.]cc	Website giả mạo Công ty Tài chính TNHH HD SAISON
7	https://hdsaison-app[.]vip	Website giả mạo Công ty Tài chính TNHH HD SAISON
8	https://www[.]hdsaison-app[.]vip	Website giả mạo Công ty Tài chính TNHH HD SAISON
9	https://www[.]hdsaison-com[.]cc	Website giả mạo Công ty Tài chính TNHH HD SAISON
10	https://www[.]hdsaison-hi[.]cc	Website giả mạo Công ty Tài chính TNHH HD SAISON
11	https://www[.]hdsaison-vn[.]cc	Website giả mạo Công ty Tài chính TNHH HD SAISON
12	https://www[.]hdsaison-vip[.]cc	Website giả mạo Công ty Tài chính TNHH HD SAISON
13	https://www[.]hdsaison-vn[.]com	Website giả mạo Công ty Tài chính TNHH HD SAISON

14	https://www[.]hdsaison[.]cc	Website giả mạo Công ty Tài chính TNHH HD SAISON
15	https://www[.]hdsaison-app[.]cc	Website giả mạo Công ty Tài chính TNHH HD SAISON
16	https://hdsaison-vip[.]cc	Website giả mạo Công ty Tài chính TNHH HD SAISON
17	https://hdsaison-hi[.]cc	Website giả mạo Công ty Tài chính TNHH HD SAISON
18	https://hdsaison-com[.]cc	Website giả mạo Công ty Tài chính TNHH HD SAISON
19	https://hdsaison-vn[.]cc	Website giả mạo Công ty Tài chính TNHH HD SAISON
20	https://hdsaison-app[.]vip	Website giả mạo Công ty Tài chính TNHH HD SAISON
21	https://hdsaison-app[.]cc	Website giả mạo Công ty Tài chính TNHH HD SAISON
22	https://hdsaison[.]cc	Website giả mạo Công ty Tài chính TNHH HD SAISON
23	https://aeshopvn[.]com	Website giả mạo Công ty TNHH Aeon Việt Nam
24	https://dichvucong[.]cvgov[.]com	Website giả mạo Dịch vụ công Quốc Gia
25	https://dichvucong[.]xgovn[.]net	Website giả mạo Dịch vụ công Quốc Gia
26	https://dichvucong[.]dulieuquocgia[.]com	Website giả mạo Dịch vụ công Quốc Gia
27	https://dienmayxanh263[.]com	Website giả mạo Điện máy xanh
28	https://etkf44[.]com	Website giả mạo Điện máy xanh
29	https://etkf44[.]com	Website giả mạo Điện máy xanh
30	https://vuabem[.]com	Website giả mạo Momo

31	https://trumbem[.]com	Website giả mạo Momo
32	https://www[.]abb-vnbank[.]cc	Website giả mạo Ngân hàng TMCP An Bình
33	https://baoviet-vn[.]cc	Website giả mạo Ngân hàng TMCP Bảo VIệt
34	https://baoviet-vn[.]cc	Website giả mạo Ngân hàng TMCP Bảo Việt
35	https://khcn-han-muc-tin-dung-ca-nhan[.]com	Website giả mạo Ngân hàng TMCP Hàng hải Việt Nam
36	https://nganhangsaison[.]org/	Website giả mạo Ngân hàng TMCP Phát triển Thành phố Hồ Chí Minh
37	https://mothe[.]tindung-hd[.]com	Website giả mạo Ngân hàng TMCP Phát triển Thành phố Hồ Chí Minh
38	https://cskhmbcanhan[.]com	Website giả mạo Ngân hàng TMCP Quân đội
39	https://cskhmbcanhan[.]com	Website giả mạo Ngân hàng TMCP Quân đội
40	https://cskh-vib[.]ho-tro-tin-dung-ca-nhan[.]com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
41	https://dich-vu-xvip-vib[.]com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
42	https://dich-vu-vip3-vib[.]com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
43	https://dich-vu-the-vdiamond-vib[.]com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
44	https://cskh-vib-canhan[.]com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
45	https://dich-vu-the-cashback-vib[.]com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
46	https://dich-vu-the-kt3-vib[.]com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam

47	http://vib[.]tructuyen-chamsockhachang-the[.]com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
48	https://bio[.]linkvibthetindung	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
49	https://vib[.]chamsocthekhachang-tructuyen[.]com[.]vn	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
50	https://nang-cap-hang-vvip-vib[.]com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
51	https://vib[.]chamsocthekhachang-tructuyen[.]com[.]vn	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
52	https://nanghanmucthevib[.]com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
53	https://scb[.]chamsockhachhang-truc-tuyen-the[.]online	Website giả mạo Ngân hàng TMCP Sài Gòn
54	https://tpbank[.]chamsocthekhachang-truc-tuyen[.]com/	Website giả mạo Ngân hàng TMCP Tiên Phong
55	https://cskh-ca-nhan-vpbank[.]com	Website giả mạo Ngân hàng TMCP Việt Nam Thịnh Vượng
56	https://dich-vu-update-vpbank[.]com	Website giả mạo Ngân hàng TMCP Việt Nam Thịnh Vượng
57	https://cskh-ca-nhan-vpbank[.]com	Website giả mạo Ngân hàng TMCP Việt Nam Thịnh Vượng
58	https://nang-cap-vip-vpbank[.]com	Website giả mạo Ngân hàng TMCP Việt Nam Thịnh Vượng
59	https://dv-ca-nhan-vpbank[.]com	Website giả mạo Ngân hàng TMCP Việt Nam Thịnh Vượng
60	https://dv-ca-nhan-vpbank[.]com	Website giả mạo Ngân hàng TMCP Việt Nam Thịnh Vượng
61	https://shinhan[.]ho-tro-tin-dung-ca-nhan[.]com	Website giả mạo Ngân hàng TNHH MTV Shinhan Việt Nam
62	https://www[.]amadbfk[.]shop	Website giả mạo sàn TMĐT Amazon
63	https://www[.]amajwzon456[.]top	Website giả mạo sàn TMĐT Amazon

64	https://www[.]jneolvsg0lm9hwkb[.]cc	Website giả mạo sàn TMĐT Amazon
65	https://ebayget[.]cc	Website giả mạo sàn TMĐT Ebay
66	https://lzd2024[.]com	Website giả mạo sàn TMĐT Lazada
67	https://sendovn[.]com	Website giả mạo sàn TMĐT Sendo
68	https://vnsendo[.]vip	Website giả mạo sàn TMĐT Sendo
69	https://vn78223p[.]com	Website giả mạo sàn TMĐT Shopee
70	https://vn86414s[.]com	Website giả mạo sàn TMĐT Shopee
71	https://soppe68[.]com	Website giả mạo sàn TMĐT Shopee
72	https://vn88631p[.]com	Website giả mạo sàn TMĐT Shopee
73	https://spmail86[.]com	Website giả mạo sàn TMĐT Shopee
74	https://spmail88[.]com	Website giả mạo sàn TMĐT Shopee
75	https://s33788[.]com/	Website giả mạo sàn TMĐT Shopee
76	https://vn667755s[.]com/login	Website giả mạo sàn TMĐT Shopee
77	https://vn55779p[.]com	Website giả mạo sàn TMĐT Shopee
78	https://www[.]ssvnshop[.]com	Website giả mạo sàn TMĐT Shopee
79	https://sp63899vn[.]com	Website giả mạo sàn TMĐT Shopee
80	https://vn11568p[.]com	Website giả mạo sàn TMĐT Shopee

81	https://www[.]shopeesmarket[.]com	Website giả mạo sàn TMĐT Shopee
82	https://tdkd01[.]com	Website giả mạo sàn TMĐT Tiki
83	https://eufk55[.]com	Website giả mạo sàn TMĐT Tiki
84	https://tikimall[.]org	Website giả mạo sàn TMĐT Tiki
85	https://hgff11[.]com	Website giả mạo sàn TMĐT Tiki
86	https://ghnn22[.]com	Website giả mạo sàn TMĐT Tiki
86	https://ghnn11[.]com	Website giả mạo sàn TMĐT Tiki
88	https://ghnn33[.]com	Website giả mạo sàn TMĐT Tiki
89	https://tiki98[.]com	Website giả mạo sàn TMĐT Tiki
90	Http://tdkd03[.]com	Website giả mạo sàn TMĐT Tiki
91	https://tdkd03[.]com	Website giả mạo sàn TMĐT Tiki
92	https://tdkd03[.]com	Website giả mạo sàn TMĐT Tiki
93	Http://tdkd03[.]com	Website giả mạo sàn TMĐT Tiki
94	https://zla963[.]top	Website giả mạo sàn TMĐT Tiki
95	https://dadw22[.]com	Website giả mạo sàn TMĐT Tiki
96	https://dadw11[.]com	Website giả mạo sàn TMĐT Tiki
97	https://tah0a[.]com	Website giả mạo sàn TMĐT Tiki

98	https://tikivn[.]in	Website giả mạo sàn TMĐT Tiki
99	https://dadw55[.]com	Website giả mạo sàn TMĐT Tiki
100	https://viettelgroupvn[.]com	Website giả mạo Viettel

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	16949	https://nvd.nist.gov/vuln/detail/ CVE-2022-26809
2	CVE-2024-2176	8962	https://nvd.nist.gov/vuln/detail/ CVE-2024-2176
3	CVE-2024-2631	8723	https://nvd.nist.gov/vuln/detail/ CVE-2024-2631
4	CVE-2023-21716	7861	https://nvd.nist.gov/vuln/detail/ CVE-2023-21716
5	CVE-2024-1939	7379	https://nvd.nist.gov/vuln/detail/ CVE-2024-1939
6	CVE-2024-2400	6746	https://nvd.nist.gov/vuln/detail/ CVE-2024-2400
7	CVE-2024-26197	4914	https://nvd.nist.gov/vuln/detail/ CVE-2024-26197
8	CVE-2024-25858	4848	https://nvd.nist.gov/vuln/detail/ CVE-2024-25858
9	CVE-2024-1676	4212	https://nvd.nist.gov/vuln/detail/ CVE-2024-1676
10	CVE-2024-29944	2370	https://nvd.nist.gov/vuln/detail/ CVE-2024-29944

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	STT	Indicators of compromise
1	differentia[.]ru	14	update[.]microsoft-setting[.]com
2	update[.]centos-yum[.]com	15	update[.]windows[.]server-microsoft[.]com
3	update.devicebug[.]com	16	149[.]28[.]26[.]2
4	23[.]106[.]124[.]152	17	cdn-dev[.]helpkaspersky[.]top
5	115[.]126[.]98[.]204	18	data-dev[.]helpkaspersky[.]top
6	118[.]99[.]6[.]202	19	happy[.]gitweb[.]cloudns[.]nz
7	199[.]231[.]211[.]19	20	support[.]helpkaspersky[.]top
8	www[.]security-microsoft[.]net	21	softupdate[.]xyz
9	gtldgtld[.]store	22	122.10.90[.]12
10	tfirstdaily[.]store	23	C3DBEEB5B9339E62FA9300F4E3BBC89D
11	ruuovqsbhnqvvnekx[.]org	24	07F85171FFA199899EC0B7136F164986
12	getfilefox[.]com	25	AE9601C8A66D41828795A3F6CCE31B19
13	54.180.143[.]194	26	437890563718E151BEFB3E44AC6DD5B1