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: 8 /BC-CATTT

Hà Nội, ngày 07 tháng 05 năm 2024

BÁO CÁO AN TOÀN THÔNG TIN MẠNG VIỆT NAM
(Tháng 4/2024)

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 **4/2024**, 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.

Trong tháng **4/2024**, 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.

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 15 hàng tháng**.

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

Văn bản số 364/CATTT-NCSC về việc lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 03/2024 phát hành ngày 15/03/2024.

Văn bản số 607/CATTT-NCSC về việc lỗ hổng bảo mật ảnh hưởng nghiêm trọng trong phần mềm PAN-OS phát hành ngày 17/04/2024.

Văn bản số 722/CATTT-NCSC về việc cảnh báo phát hiện mã độc trojan Redline Stealer gây ảnh hưởng trên các hệ thống thông tin phát hành ngày 24/04/2024.

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 **124.624 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 **4/2024**, hệ thống của NCSC đã phát hiện **42 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 **89.351** 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 **4/2024**, 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 4/2024:

TT	Mã điểm yếu/lỗ hổng	Mô tả	Ghi chú
1	CVE-2024-3094	- Điểm CVSS: 10.0 (Nghiêm trọng) - Mô tả: Lỗ hổng cho phép đối tượng tấn công truy cập và thực hiện các hành vi trái phép. - Ảnh hưởng: Tukaani XZ - Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.	https://nvd.nist.gov/vuln/detail/CVE-2024-3094
2	CVE-2024-21894	- 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 tùy ý. - Ảnh hưởng: Ivanti Connect Secure, vanti Policy Secure - Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế	https://nvd.nist.gov/vuln/detail/CVE-2024-21894
3	CVE-2024-3400	- Điểm CVSS: 10 (Nghiêm trọng - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã tùy ý. - Ảnh hưởng: Palo Alto Networks PAN-OS	https://nvd.nist.gov/vuln/detail/CVE-2024-3400

		- Lỗ hổng đã có mã khai thác và hiện đang bị khai thác trong thực tế.	
4	CVE-2024-20720	- Điểm CVSS: 8.2 (Nghiêm trọng) - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã tùy ý trên hệ thống. - Ảnh hưởng: Adobe Commerce - Lỗ hổng đã có mã khai thác và hiện đang bị khai thác trong thực tế.	https://nvd.nist.gov/vuln/detail/CVE-2024-20720
5	CVE-2023-46805	- Điểm CVSS: 8.2 (Cao) - Mô tả: Lỗ hổng cho phép đối tượng tấn công bỏ qua bảo mật xác thực. - Ảnh hưởng: Ivanti ICS. - Lỗ hổng đã có mã khai thác và hiện đang bị khai thác trong thực tế.	https://nvd.nist.gov/vuln/detail/ CVE-2023-46805
6	CVE-2024-21887	- Điểm CVSS: 9.1 (Nghiêm trọng) - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã tùy ý. - Ảnh hưởng: Ivanti Connect Secure, Ivanti Policy Secure - Lỗ hổng đã có mã khai thác và hiện đang bị khai thác trong thực tế.	https://nvd.nist.gov/vuln/detail/CVE-2024-21887
7	CVE-2024-20359	- Điểm CVSS: 6.0 (Trung bình) - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã tùy ý. - Ảnh hưởng: Cisco Adaptive Security Appliance (ASA), Cisco Firepower Threat Defense (FTD). - Lỗ hổng đã có mã khai thác và hiện đang bị khai thác trong thực tế.	https://nvd.nist.gov/vuln/detail/ CVE-2024-20359
8	CVE-2024-2879	- Điểm CVSS: 7.5 (Cao) - 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 và hiện đang bị khai thác trong thực tế.	https://nvd.nist.gov/vuln/detail/ CVE-2024-2879

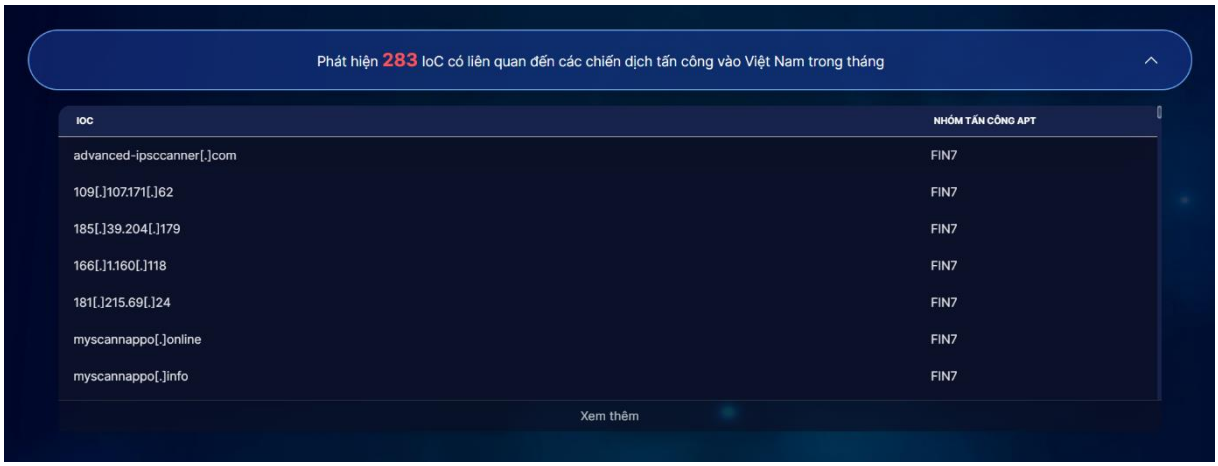
9	CVE-2024-22023	- Điểm CVSS: 5.3 (Trung bình) - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ. - Ảnh hưởng: Ivanti Connect Secure, Ivanti Policy Secure - Lỗ hổng hiện đang bị khai thác trong thực tế.	https://nvd.nist.gov/vuln/detail/ CVE-2024-22023
10	CVE-2024-22053	- Điểm CVSS: 8.2 (Cao) - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ. - Ảnh hưởng: Ivanti Connect Secure, Ivanti Policy Secure - Lỗ hổng hiện đang bị khai thác trong thực tế.	https://nvd.nist.gov/vuln/detail/CVE-2024-22053
11	CVE-2024-22052	- 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: Ivanti Connect Secure, Ivanti Policy Secure - Lỗ hổng hiện đang bị khai thác trong thực tế.	https://nvd.nist.gov/vuln/detail/CVE-2024-22052
12	CVE-2024-21893	- Điểm CVSS: 8.2 (Cao) - Mô tả: Lỗ hổng cho phép đối tượng tấn công khai thác lỗi SSRF. - Ảnh hưởng: Ivanti Connect Secure, Ivanti Policy Secure. - Lỗ hổng hiện đang bị khai thác trong thực tế.	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 607/CATTT-NCSC ngày 17/04/2024 về việc lỗ hổng bảo mật ảnh hưởng nghiêm trọng trong phần mềm PAN-OS; công văn số 722/CATTT-NCSC ngày 24/04/2024 về việc cảnh báo phát hiện mã độc trojan Redline Stealer gây ảnh hưởng trên các 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.



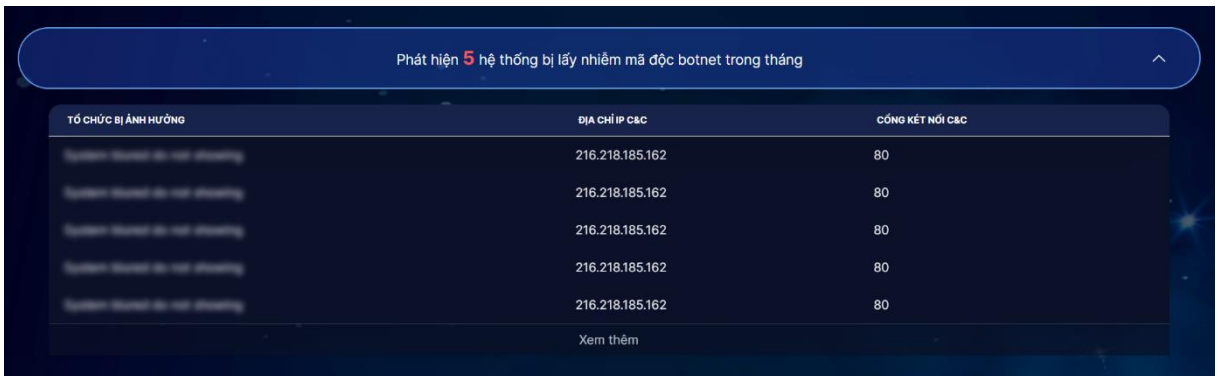
Thông tin IOC được cung cấp tại https://alert.khonggianmang.vn/

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 **4/2024**, Trung tâm NCSC phát hiện **05 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.*

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

Trần Đăng Khoa

Phụ lục I

DANH SÁCH CÁC WEBSITE GIẢ MẠO, LỪA ĐẢO PHÁT HIỆN TRONG THÁNG

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

TT	Website giả mạo	Ghi chú
1	https://www[.]vnambzuon36sc[.]vip/	Website giả mạo sàn TMĐT Amazon
2	https://vn147258p[.]com	Website giả mạo sàn TMĐT Amazon
3	https://quaysomediamart2024[.]vip	Website giả mạo Công ty Cổ phần MediaMart Việt Nam
4	https://quaysomediamart2024[.]vip/	Website giả mạo Công ty Cổ phần MediaMart Việt Nam
5	https://hdtinchap[.]com	Website giả mạo Công ty Tài chính TNHH HD SAISON
6	https://mayxanhsupport[.]com/	Website giả mạo Điện máy xanh
7	https://lotttemart[.]store	Website giả mạo LOTTE
8	https://clzl[.]pro	Website giả mạo MoMo
9	https://vdbank[.]com[.]vn	Website giả mạo Ngân hàng Phát triển Việt Nam
10	https://sotuyenvcb[.]vietcombanker[.]com	Website giả mạo Ngân Hàng TMCP Ngoại thương Việt Nam
11	https://mbfic-plus[.]com	Website giả mạo Ngân hàng TMCP Quân đội
12	https://khach-hang-ca-nhan-vip5[.]com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
13	https://dich-vu-khcn-vvip-vib[.]com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam

14	cskh-vib[.]nang-han-muc-the-visa[.]com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
15	khcn-uu-tien-3fv-vib[.]com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
16	kh-cn-uutien-3fv-vib[.]com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
17	stcard-vib[.]com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
18	https://khachhangvib-canhan[.]com/	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
19	https://vibbca-nhan[.]com/	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
20	https://nang-han-muc-vcs1-khcn-vib[.]com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
21	http://vipcard-vib[.]com/	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
22	https://khoi-khach-hang-ca-nhan-vni-diamon[.]com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
23	https://vpb[.]tanghanmucvisa-vn[.]com	Website giả mạo Ngân hàng TMCP Việt Nam Thịnh Vượng
24	https://shinhan[.]chamsoccanhankhachhangthe-tructuyen[.]online	Website giả mạo Ngân hàng TNHH MTV Shinhan Việt Nam
25	https://canhanshinhan[.]com	Website giả mạo Ngân hàng TNHH MTV Shinhan Việt Nam
26	https://vnsendo[.]shop/	Website giả mạo sàn TMĐT Sendo
27	https://www[.]dailyssshopee[.]com	Website giả mạo sàn TMĐT Shopee
28	https://vn63251s[.]com	Website giả mạo sàn TMĐT Shopee
29	https://vn68822s[.]com/	Website giả mạo sàn TMĐT Shopee
30	https://sp77888[.]com/	Website giả mạo sàn TMĐT Shopee

31	http://sp6788[.]com	Website giả mạo sàn TMĐT Shopee
32	https://sp56788[.]com/	Website giả mạo sàn TMĐT Shopee
33	https://investshopeemall[.]net/	Website giả mạo sàn TMĐT Shopee
34	https://skhf11[.]com	Website giả mạo sàn TMĐT Tiki
35	https://fdsd22[.]com	Website giả mạo sàn TMĐT Tiki
36	https://www[.]tuyendungtiki2024[.]vn/	Website giả mạo sàn TMĐT Tiki
37	https://tdkd00[.]com/	Website giả mạo sàn TMĐT Tiki
38	https://fdsd11[.]com/	Website giả mạo sàn TMĐT Tiki
39	https://nhanvientiki[.]info/	Website giả mạo sàn TMĐT Tiki
40	https://skhf66[.]com/	Website giả mạo sàn TMĐT Tiki
41	https://tdkd07[.]com	Website giả mạo sàn TMĐT Tiki
42	https://tdkd08[.]com/	Website giả mạo sàn TMĐT Tiki

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	15934	https://nvd.nist.gov/vuln/detail/ CVE-2022-26809
2	CVE-2024-3516	11294	https://nvd.nist.gov/vuln/detail/ CVE-2024-3516
3	CVE-2024-3914	10154	https://nvd.nist.gov/vuln/detail/ CVE-2024-3914
4	CVE-2024-2887	8555	https://nvd.nist.gov/vuln/detail/ CVE-2023-2887
5	CVE-2023-21716	6598	https://nvd.nist.gov/vuln/detail/ CVE-2024-21716
6	CVE-2024-4060	5045	https://nvd.nist.gov/vuln/detail/ CVE-2024-4060
7	CVE-2024-3865	3406	https://nvd.nist.gov/vuln/detail/ CVE-2024-3965
8	CVE-2024-3846	3346	https://nvd.nist.gov/vuln/detail/ CVE-2024-3846
9	CVE-2024-3159	2871	https://nvd.nist.gov/vuln/detail/ CVE-2024-2871
10	CVE-2022-0001	2771	https://nvd.nist.gov/vuln/detail/ CVE-2024-2771

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	Update.py	CVE-2024-3400
2	3de2a4392b8715bad070b2ae12243f166ead37830f7c6d24e778985927f9caac	
3	5460b51da26c060727d128f3b3d6415d1a4c25af6a29fef4cc6b867ad3659078	
4	172.233.228[.]93	
5	hxxp://172.233.228[.]93/policy	
6	hxxp://172.233.228[.]93/patch	
7	66.235.168[.]222	
8	5e37b3289054d5e774c02a6ec4915a60156d715f3a02aaceb7256cc3ebdc6610	Redline Stealer
9	https[:]//github[.]com/microsoft/vcpkg/files/14125503/Cheat.Lab.2.7.2.zip	
10	873aa2e88dbc2efa089e6efd1c8a5370e04c9f5749d7631f2912bcb640439997	
11	751f97824cd211ae710655e60a26885cd79974f0f0a5e4e582e3b635492b4cad	
12	dfbf23697cfd9d35f263af7a455351480920a95bfc642f3254ee8452ce20655a	
13	213[.]248[.]43[.]58	
14	hxxps://github.com/microsoft/STL/files/14432565/Cheater.Pro.1.6.0.zip	

15	51[.]79[.]208[.]192	CoralRaider
16	199[.]34[.]27[.]196	
17	139[.]99[.]23[.]9	
18	14[.]225[.]210[.]98	
19	14[.]225[.]210[.]97	
20	14[.]225[.]210[.]209	
21	14[.]225[.]210[.]222	
22	doc-0s-44-docstext[.]googleusercontent[.]com	
23	doc-10-44-docstext[.]googleusercontent[.]com	
24	kzeight8ht.top/upload.php	
25	kbeight8sb.top/upload.php	
26	kbeight8vs.top/upload.php	
27	kbeight8ht.top/upload.php	
28	kbeight8pn.top/upload.php	
29	dbeight8pt.top/zip.php	
30	kveight8sb.top/zip.php	
31	peasanthovecapspll.shop/api	
32	claimconcessionrebe.shop/api	
33	culturesketchfinanciall.shop/api	
34	gemcreedarticulateod.shop/api	
35	liabilityarrangemenyit.shop/api	
36	modestessayevenmilwek.shop/api	
37	secretionsuitcasenioise.shop/api	
38	sofahuntingslidedine.shop/api	
39	triangleseasonbenchwj.shop/api	
40	185.23.108.220|6339	
41	techsheck.b-cdn.net/Zen90	
42	zexodown-2.b-cdn.net/Peta12	
43	denv-2.b-cdn.net/FebL5	
44	metrodown-2.b-cdn.net/MebL1	
45	metrodown-2.b-cdn.net/SAq2	
46	denv-2.b-cdn.net/FebL4	

47	download-main5.b-cdn.net/BSR_v7IDcc	
48	metrodown-3.b-cdn.net/MebL1	
49	dashdisk-2.b-cdn.net/XFeb18	
50	103.27.202[.]85	ToddyCat
51	118.193.40[.]42	
52	Ha[.]bbmouseme[.]com	
53	192.36.57[.]181	UAT4356
54	185.227.111[.]17	
55	172.105.90[.]154	
56	45.86.163[.]224	
57	213.156.138[.]77	
58	45.77.52[.]253	
59	212.193.2[.]48	
60	89.44.198[.]196	
61	213.156.138[.]78	
62	213.156.138[.]68	
63	185.244.210[.]65	
64	185.167.60[.]85	
65	176.31.18[.]153	
66	185.244.210[.]120	
67	172.105.94[.]93	
68	89.44.198[.]189	
69	103.114.200[.]230	
70	51.15.145[.]37	
71	131.196.252[.]148	
72	121.227.168[.]69	
73	194.4.49[.]6	
74	216.238.75[.]155	