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: /BC-CATTT

Hà Nội, ngày tháng năm 2024

BÁO CÁO AN TOÀN THÔNG TIN MẠNG VIỆT NAM
(Tháng 5/2024)

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 **5/2024**, 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 **5/2024**, 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 25/6/2024.**

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

Văn bản số 884/CATTT-NCSC về việc lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 4/2024 phát hành ngày 16/5/2024.

Văn bản số 764/CATTT-NCSC về việc cảnh báo chiến dịch tấn công mới nhằm vào các thiết bị mạng Cisco phát hành ngày 03/5/2024.

Văn bản số 950/CATTT-NCSC về việc cảnh báo chiến dịch tấn công sử dụng mã độc RAT để thực hiện hành vi trái phép phát hành ngày 27/5/2024.

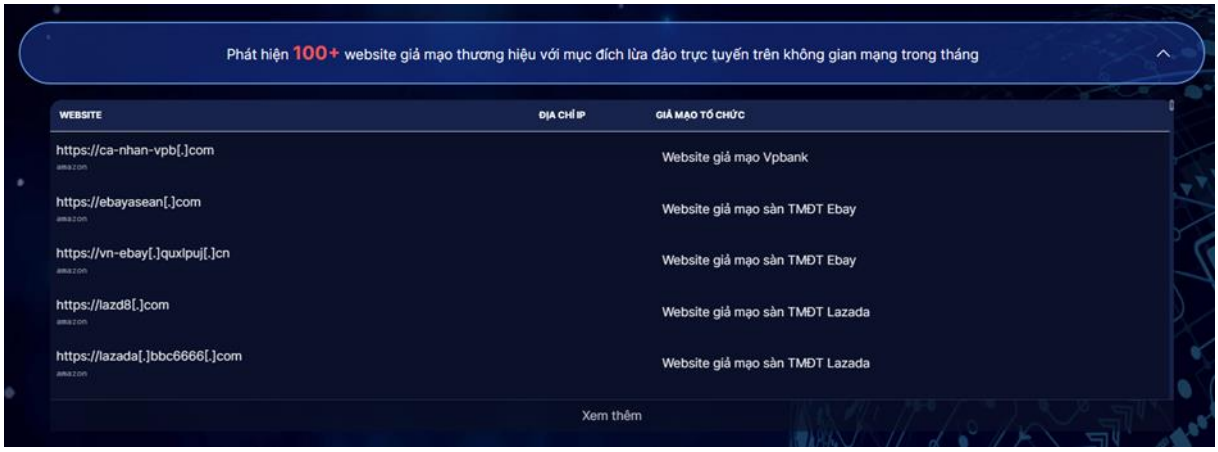
Văn bản số 995/CATTT-NCSC về việc cảnh báo lỗ hổng an toàn thông tin CVE-2024-24919 tồn tại trên các sản phẩm của hãng Check Point phát hành ngày 31/5/2024.

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 **124.775 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 **5/2024**, hệ thống của NCSC đã phát hiện **71 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/

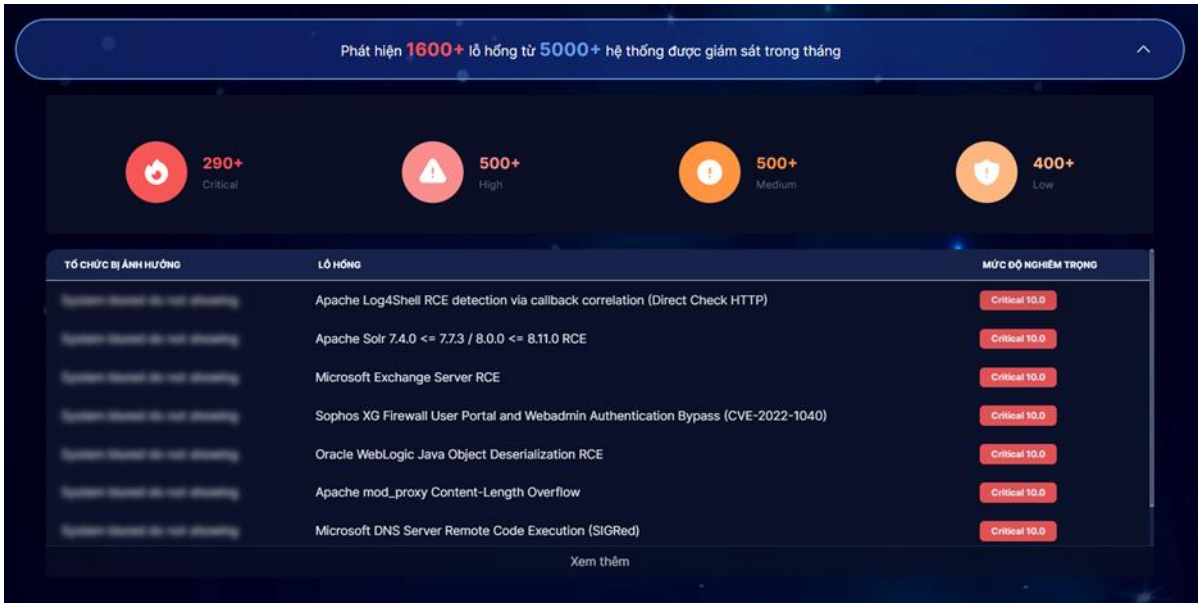
Ghi chú: *Danh sách các website giả mạo đã phát hiện tại Phụ lục I kèm theo.*

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 **5/2024**, 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 5/2024:

TT	Mã điểm yếu/lỗ hổng	Mô tả	Ghi chú
1	CVE-2024-4671	- Điểm CVSS: 9.6 (Nghiêm trọng) - Mô tả: Lỗ hổng cho phép đối tượng tấn công sử dụng trang HTML độc hại để khai thác lỗ hổng use after free trong Visuals của Google Chrome, qua đó có thể thoát khỏi môi trường phân tích sandbox.	https://nvd.nist.gov/vuln/detail/CVE-2024-4671

		- Ảnh hưởng: Google Chrome - Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.	
2	CVE-2024-32002	- Điểm CVSS: 9.0 (Nghiêm trọng) - Mô tả: Lỗ hổng cho phép đối tượng tấn công truy cập và thực hiện các hành vi trái phép. - Ảnh hưởng: Git. - Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.	https://nvd.nist.gov/vuln/detail/CVE-2024-32002
3	CVE-2024-4761	- Điểm CVSS: 8.8 (Cao) - Mô tả: Lỗ hổng ghi out-of-bounds cho phép đối tượng tấn công truy cập và thực hiện các hành vi trái phép. - Ảnh hưởng: Google Chrome. - Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.	https://nvd.nist.gov/vuln/detail/CVE-2024-4761
4	CVE-2024-4040	- Điểm CVSS: 10.0 (Nghiêm trọng) - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã từ xa, truy cập và thực hiện các hành vi trái phép. - Ảnh hưởng: CrushFTP - Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.	https://nvd.nist.gov/vuln/detail/CVE-2024-4040
5	CVE-2024-21187	- Điểm CVSS: 9.1 (Nghiêm trọng) - Mô tả: Ivanti Connect Secure, Ivanti Policy Secure. - Ảnh hưởng: Lỗ hổng cho phép đối tượng tấn công thực thi mã từ xa. - Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.	https://nvd.nist.gov/vuln/detail/CVE-2024-21887

6	CVE-2024-3400	- Điểm CVSS: 10.0 (Nghiêm trọng) - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực hiện command injection, từ đó dẫn tới thực thi mã từ xa. - 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-2024-3400
7	CVE-2024-4947	- Điểm CVSS: 8.8 (Cao) - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã tùy ý trong môi trường phân tích sandbox. - Ảnh hưởng: Google Chrome. - Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.	https://nvd.nist.gov/vuln/detail/CVE-2024-4947
8	CVE-2024-21111	- Điểm CVSS: 7.8 (Cao) - Mô tả: Lỗ hổng cho phép đối tượng tấn truy cập và thực hiện các hành vi trái phép. - Ảnh hưởng: Oracle VM VirtualBox - Lỗ hổng đang bị khai thác trong thực tế.	https://nvd.nist.gov/vuln/detail/CVE-2024-21111
9	CVE-2024-21683	- Điểm CVSS: 8.8 (Cao) - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Confluence Data Center, Confluence Server - Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.	https://nvd.nist.gov/vuln/detail/CVE-2024-21683
10	CVE-2024-4367	- Điểm CVSS: 7.5 (Cao) - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã JavaScript từ xa.	https://nvd.nist.gov/vuln/detail/CVE-2024-4367

		- Ảnh hưởng: Mozilla Firefox, Mozilla Firefox ESR, Mozilla Thunderbird. - Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.	
11	CVE-2024-30051	- Điểm CVSS: 7.8 (Cao) - Mô tả: Lỗ hổng cho phép đối tượng tấn công leo thang đặc quyền. - Ảnh hưởng: Microsoft Windows 10, Windows 11. - Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.	https://nvd.nist.gov/vuln/detail/CVE-2024-30051
12	CVE-2024-27322	- Điểm CVSS: 8.8 (Cao) - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã tùy ý. - Ảnh hưởng: Ngôn ngữ lập trình R - Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.	https://nvd.nist.gov/vuln/detail/CVE-2024-27322

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 764/CATTT-NCSC ngày 03/5/2024 về việc cảnh báo chiến dịch tấn công mới nhằm vào các thiết bị mạng Cisco; Công văn số 950/CATTT-NCSC ngày 27/5/2024 về việc cảnh báo chiến dịch tấn công sử dụng mã độc RAT để thực hiện hành vi trái phép; Công văn số 995/CATTT-NCSC ngày 31/5/2024 về việc cảnh báo lỗ hổng an toàn thông tin CVE-2024-24919 tồn tại trên các sản phẩm của hãng Check Point.

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 **5/2024**, 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.

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 (để b/c);
- Phó Cục trưởng Trần Đăng Khoa;
- Các phòng: ATHTTT, TT&HTQT;
- Trung tâm VNCERT/CC;
- Lưu: VT, NCSC.LTQ.

KT. CỤC TRƯỞNG
PHÓ CỤC TRƯỞNG

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[.]amazonl0[.]com/	Website giả mạo sàn TMĐT Amazon
2	https://miaoniter[.]com/	Website giả mạo sàn TMĐT Amazon
3	https://amazonl3[.]com/	Website giả mạo sàn TMĐT Amazon
4	https://www[.]amatvip36sc[.]cc/	Website giả mạo sàn TMĐT Amazon
5	https://vssid[.]cc/	Website giả mạo Bảo hiểm Xã hội Việt Nam
6	https://bachoaxanhh[.]com	Website giả mạo Công ty cổ phần Thương mại Bách Hóa Xanh
7	https://homecreditvn[.]net	Website giả mạo Công ty Tài chính TNHH MTV Home Credit Việt Nam
8	https://aeeonmaili[.]shop/	Website giả mạo Công ty TNHH Aeon Việt Nam
9	https://dienmayxanh542[.]com	Website giả mạo Điện máy xanh
10	https://dich-vu-dien-mayxanh[.]com	Website giả mạo Điện máy xanh
11	https://trungtam-dienmayxanh[.]com	Website giả mạo Điện máy xanh
12	https://c[.]vn-ebayn[.]vip	Website giả mạo sàn TMĐT Ebay

13	https://ebayasean[.]com	Website giả mạo sàn TMĐT Ebay
14	https://vn-ebay[.]quxlpuj[.]cn/	Website giả mạo sàn TMĐT Ebay
15	https://lazd8[.]com	Website giả mạo sàn TMĐT Lazada
16	https://lazada[.]bbc6666[.]com	Website giả mạo sàn TMĐT Lazada
17	https://www[.]hethongdonhang[.]com/	Website giả mạo sàn TMĐT Lazada
18	https://la7890[.]cc/	Website giả mạo sàn TMĐT Lazada
19	https://da6555[.]com/	Website giả mạo sàn TMĐT Lazada
20	https://da2323[.]com	Website giả mạo sàn TMĐT Lazada
21	https://khoi-khach-hang-ca-nhan-uu-tien-vni[.]com/	Website giả mạo Mbbank
22	https://mbfn-fic[.]com/	Website giả mạo Mbbank
23	https://mbcanhan-cskh[.]com/	Website giả mạo Mbbank
24	https://www[.]mbdkb[.]com/	Website giả mạo Mbbank
25	https://phattai247[.]com/	Website giả mạo Mbbank
26	http://vieetcombiank[.]com	Website giả mạo Ngân Hàng TMCP Ngoại thương Việt Nam
27	https://tinchaphd[.]com/	Website giả mạo Ngân hàng TMCP Phát triển Thành phố Hồ Chí Minh
28	hdb[.]vntanghanmucvisadebit[.]com	Website giả mạo Ngân hàng TMCP Phát triển Thành phố Hồ Chí Minh

29	hdb[.]tang-han-muc-tin-dung-vn[.]com	Website giả mạo Ngân hàng TMCP Phát triển Thành phố Hồ Chí Minh
30	https://ocb[.]chamsocthekhachhang-uudai-tructuyen[.]com/	Website giả mạo Ngân hàng TMCP Phương Đông
31	https://finacehoisomb[.]com	Website giả mạo Ngân hàng TMCP Quân đội
32	https://mbdkb[.]com	Website giả mạo Ngân hàng TMCP Quân đội
33	https://visa-mb[.]com	Website giả mạo Ngân hàng TMCP Quân đội
34	https://khoi-khach-hang-ca-nhan-vni-diamon[.]com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
35	http://vib[.]tanghanmuc-vn[.]com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
36	http://vib[.]hanmucvn[.]com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
37	https://han-muc-khcn-uu-tien-vna1[.]com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
38	khcn-my-diamon-han-muc-uu-tien[.]com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
39	vib-mydiamon-khcn-uutien-vnc1[.]com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
40	https://mydiamon-han-muc-ca-nhan-vni[.]com/	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
41	vib[.]chamsocuudaithekhachhang-tructuyen[.]com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
42	vib[.]chamsockhachhangtheuudai-tructuyen[.]com[.]vn	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
43	https://khvib-canhan[.]com/	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
44	kh-vibquocte[.]com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam

45	http://mail[.]labtpb[.]online	Website giả mạo Ngân hàng TMCP Tiên Phong
46	https://canhantpb[.]com	Website giả mạo Ngân hàng TMCP Tiên Phong
47	https://tpbank[.]chamsockhachhang-uudaitructuyen[.]online	Website giả mạo Ngân hàng TMCP Tiên Phong
48	kh-cn-mrd-f5-tpbank[.]com	Website giả mạo Ngân hàng TMCP Tiên Phong
49	https://tpbankvn[.]workplace[.]com	Website giả mạo Ngân hàng TMCP Tiên Phong
50	https://tpb-vayuudai[.]com/	Website giả mạo Ngân hàng TMCP Tiên Phong
51	https://vpb[.]tanghanmucvisa-vn[.]com	Website giả mạo Ngân hàng TMCP Việt Nam Thịnh Vượng
52	http://vpb[.]tang-han-muc-the-visa-vn[.]com	Website giả mạo Ngân hàng TMCP Việt Nam Thịnh Vượng
53	vpb[.]nanghanmucvisa-vn[.]com	Website giả mạo Ngân hàng TMCP Việt Nam Thịnh Vượng
54	https://miles-card-vpbank[.]com	Website giả mạo Ngân hàng TMCP Việt Nam Thịnh Vượng
55	https://shinhan[.]chamsocthekhachhang-thang4[.]online	Website giả mạo Ngân hàng TNHH MTV Shinhan Việt Nam
56	https://shinhanbank[.]vnfiba[.]com	Website giả mạo Ngân hàng TNHH MTV Shinhan Việt Nam
57	https://vnsendo[.]shop/	Website giả mạo sàn TMĐT Sendo
58	https://vnsendo[.]info	Website giả mạo sàn TMĐT Sendo
59	https://vnsendo[.]net/	Website giả mạo sàn TMĐT Sendo
60	https://www[.]vnsendo[.]net/	Website giả mạo sàn TMĐT Sendo
61	https://investshopeemall[.]net/	Website giả mạo sàn TMĐT Sendo

62	https://sp56788[.]com/	Website giả mạo sàn TMĐT Shopee
63	https://sp5188[.]com	Website giả mạo sàn TMĐT Shopee
64	https://www[.]shopee123[.]vip	Website giả mạo sàn TMĐT Shopee
65	https://soppe68[.]shop/	Website giả mạo sàn TMĐT Shopee
66	https://sp15569p[.]com/	Website giả mạo sàn TMĐT Shopee
67	https://tdkd08[.]com/	Website giả mạo sàn TMĐT Tiki
68	https://tdkt01[.]com/	Website giả mạo sàn TMĐT Tiki
69	https://vntiki11[.]com/	Website giả mạo sàn TMĐT Tiki
70	https://dich-vu-kh-vip-vpbank[.]com/	Website giả mạo Vpbank
71	https://ca-nhan-vpb[.]com/	Website giả mạo Vpbank

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	16246	https://nvd.nist.gov/vuln/detail/ CVE-2022-26809
2	CVE-2024-4060	9950	https://nvd.nist.gov/vuln/detail/ CVE-2024-4060
3	CVE-2023-21716	6822	https://nvd.nist.gov/vuln/detail/ CVE-2023-21716
4	CVE-2024-25938	5672	https://nvd.nist.gov/vuln/detail/ CVE-2024-25938
5	CVE-2024-4950	4287	https://nvd.nist.gov/vuln/detail/ CVE-2024-4950
6	CVE-2024-4671	2588	https://nvd.nist.gov/vuln/detail/ CVE-2024-4671
7	CVE-2024-4559	1661	https://nvd.nist.gov/vuln/detail/ CVE-2024-4559
8	CVE-2024-4778	1407	https://nvd.nist.gov/vuln/detail/ CVE-2024-4778
9	CVE-2024-4368	1404	https://nvd.nist.gov/vuln/detail/ CVE-2024-4368
10	CVE-2024-30051	1219	https://nvd.nist.gov/vuln/detail/ CVE-2024-30051

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	45.33.24[.]145	Nhóm APT Turla
2	65.109.179[.]67	
3	82.165.158[.]86	
4	139.162.23[.]113	
5	161.97.74[.]237	
6	212.57.35[.]174	
7	45.79.93[.]87	
8	74.50.80[.]35	
9	82.223.55[.]220	
10	158.220.102[.]80	
11	176.57.150[.]252	
12	212.57.35[.]176	
13	fc.adswt[.]com	Nhóm APT Unfading Sea Haze
14	api.simpletra[.]com	
15	auth.bitdefenderupdate[.]com	
16	dns-log.d-n-s.org[.]uk	

17	mail.theworkguyoo[.]com	
18	payroll.mywire[.]org	
19	cdn.g8z[.]net	
20	message.ooguy[.]com	
21	newy.hifiliving[.]com	
22	provider.giize[.]com	
23	upupdate.ooguy[.]com	
24	159.223.78[.]147	
25	192.153.57[.]24	
26	193.149.129[.]128	
27	139.59.107[.]49	
28	mail.simpletra[.]com	
29	bit.kozow[.]com	
30	mail.pcygphil[.]com	
31	linklab.blinklab[.]com	
32	sopho.kozow[.]com	
33	employee.mywire[.]org	
34	managS.twilightparadox[.]com	
35	spcg.lunaticfridge[.]com	

36	images.emldn[.]com	Nhóm APT Unfading Sea Haze
37	rest.redirectme[.]net	
38	167.71.199[.]105	
39	128.199.166[.]143	
40	209.97.167[.]177	
41	128.199.66[.]11	
42	152.42.198[.]152	
43	mail.adswt[.]com	
44	bitdefenderupdate[.]org	
45	mail.bomloginset[.]com	
46	link.theworkguyoo[.]com	
47	news.nevuer[.]com	
48	airst.giize[.]com	
49	dns.g8z[.]net	
50	helpdesk.fxnxs[.]com	
51	word.emldn[.]com	
52	api.bitdefenderupdate[.]org	
53	188.166.224[.]242	
54	164.92.146[.]227	

55	112.113.112[.]5	
56	45.61.137[.]109	
57	183[.]136[.]225[.]45	Nhóm APT Muddling Meerkat
58	183[.]136[.]225[.]14	

Phụ lục IV

DANH SÁCH CÁC ĐƠN VỊ CÓ ĐỊA CHỈ IP NẰM TRONG MẠNG BOTNET

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

1. Danh sách Bộ/Ngành

TT	Tên đơn vị	Số lượng IP botnet tháng 04/2024	Số lượng IP botnet tháng 05/2024	Loại mã độc/botnet
1	Viện Hàn lâm Khoa học và Công nghệ Việt Nam	1	0	

2. Danh sách Tỉnh/thành

STT	Tên đơn vị	Số lượng IP botnet tháng 04/2024	Số lượng IP botnet tháng 05/2024	Ghi chú
1	Lai Châu	1	4	Andromeda
2	Hà Nam	0	3	Andromeda
3	Thái Bình	1	2	Andromeda
4	Gia Lai	0	1	Andromeda
5	Hà Giang	0	1	Nymaim, Ranbyus
6	Hà Nội	0	1	Andromeda
7	Lạng Sơn	0	1	Andromeda
8	Nam Định	0	1	Andromeda
9	Thanh Hóa	0	1	Andromeda
10	Bà Rịa Vũng Tàu	1	0	
11	Đắk Nông	1	0	

Phụ lục V
TÌNH HÌNH KẾT NỐI, CHIA SẺ DỮ LIỆU GIÁM SÁT THEO YÊU CẦU CHỈ THỊ SỐ 14/CT-TTG NĂM 2019

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

1. Danh sách Bộ/Ngành

TT	Bộ/Ngành/Cơ quan trực thuộc Chính phủ	Thời gian bắt đầu chia sẻ dữ liệu	Thời gian gần nhất nhận được dữ liệu (tính đến 31/05/2024)
1	Bộ Công Thương	09/08/2020	31/05/2024
2	**Bộ Giáo dục và Đào tạo**	**31/08/2020**	**09/01/2024**
3	**Bộ Giao thông vận tải**	**15/05/2020**	**26/07/2023**
4	Bộ Kế hoạch và Đầu tư	20/11/2020	25/05/2024
5	Bộ Khoa học và Công nghệ	19/11/2020	30/05/2024
6	**Bộ Lao động - Thương Binh và Xã hội**	**11/12/2020**	**03/10/2023**
7	**Bộ Ngoại giao**	**24/07/2020**	**22/01/2024**
8	Bộ Nội vụ	30/07/2020	31/05/2024
9	**Bộ Nông nghiệp và Phát triển nông thôn**	**28/09/2020**	**23/02/2024**
10	Bộ Tài chính	15/12/2020	31/05/2024
11	**Bộ Tài nguyên và Môi trường**	**03/10/2020**	**01/03/2024**
12	Bộ Thông tin và Truyền thông	11/02/2022	31/05/2024
13	Bộ Tư pháp	18/03/2023	31/05/2024
14	**Bộ Văn hóa, Thể thao và Du lịch**	**20/06/2020**	**19/03/2024**
15	Bộ Xây Dựng	23/07/2020	29/05/2024
16	**Bộ Y tế**	**17/07/2020**	**14/08/2020**
17	Ngân hàng Nhà nước Việt Nam	02/07/2020	31/05/2024

18	**Thanh tra Chính phủ**	**10/11/2020**	**01/10/2023**
19	Ủy ban Dân tộc	08/10/2020	31/05/2024
20	**Văn phòng Chính phủ**	**22/09/2020**	**06/10/2022**
21	Bảo Hiểm Xã Hội	08/11/2020	30/05/2024
22	Đài Truyền hình Việt Nam	14/09/2020	31/05/2024
23	Viện Hàn Lâm KHCN	22/09/2020	14/05/2024
24	Kiểm toán Nhà nước Việt Nam	09/03/2021	25/05/2024

2. Danh sách Tỉnh/Thành

TT	Tỉnh/Thành	Thời gian bắt đầu chia sẻ dữ liệu	Thời gian gần nhất nhận được dữ liệu (tính đến 31/05/2024)
1	An Giang	30/09/2020	29/05/2024
2	Bắc Giang	21/08/2020	31/05/2024
3	Bắc Kạn	01/09/2020	31/05/2024
4	**Bạc Liêu**	**09/10/2020**	**19/07/2023**
5	Bắc Ninh	23/07/2020	31/05/2024
6	Bà Rịa - Vũng Tàu	20/07/2020	31/05/2024
7	Bến Tre	10/08/2020	31/05/2024
8	Bình Định	05/06/2020	31/05/2024
9	Bình Dương	24/04/2020	31/05/2024
10	Bình Phước	23/04/2020	31/05/2024
11	Bình Thuận	31/08/2020	31/05/2024
12	Cà Mau	15/05/2020	31/05/2024
13	Cần Thơ	13/04/2020	31/05/2024
14	Cao Bằng	14/08/2020	31/05/2024
15	Đắk Lắk	17/06/2020	31/05/2024
16	Đắk Nông	31/08/2020	31/05/2024
17	Đà Nẵng	09/06/2020	31/05/2024
18	Điện Biên	02/06/2020	31/05/2024
19	Đồng Nai	15/06/2020	28/05/2024
20	Đồng Tháp	14/07/2020	31/05/2024
21	Gia Lai	14/09/2020	31/05/2024
22	Hà Giang	18/08/2020	31/05/2024
23	**Hải Dương**	**04/09/2020**	**12/05/2022**
24	Hải Phòng	28/07/2020	31/05/2024
25	Hà Nam	22/09/2020	31/05/2024
26	Hà Nội	30/06/2020	31/05/2024
27	Hà Tĩnh	06/10/2020	31/05/2024

28	Hòa Bình	13/05/2020	31/05/2024
29	Hồ Chí Minh	26/06/2020	31/05/2024
30	**Hậu Giang**	**02/10/2020**	**02/11/2024**
31	Hưng Yên	22/05/2020	31/05/2024
32	Khánh Hòa	21/09/2020	31/05/2024
33	Kiên Giang	24/09/2020	31/05/2024
34	Kon Tum	28/09/2020	31/05/2024
35	Lai Châu	26/09/2020	31/05/2024
36	Lâm Đồng	22/10/2020	31/05/2024
37	Lạng Sơn	08/10/2020	31/05/2024
38	Lào Cai	09/07/2020	31/05/2024
39	Long An	22/07/2020	31/05/2024
40	Nam Định	21/09/2020	31/05/2024
41	Nghệ An	09/09/2020	31/05/2024
42	Ninh Bình	28/07/2020	31/05/2024
43	Ninh Thuận	01/09/2020	31/05/2024
44	**Phú Thọ**	**01/10/2020**	**07/04/2023**
45	Phú Yên	30/11/2020	31/05/2024
46	Quảng Bình	01/07/2020	31/05/2024
47	**Quảng Nam**	**14/09/2020**	**31/1/2024**
48	Quảng Ngãi	12/08/2020	31/05/2024
49	**Quảng Ninh**	**12/09/2020**	**18/11/2023**
50	Quảng Trị	24/12/2020	31/05/2024
51	Sóc Trăng	12/08/2020	31/05/2024
52	Sơn La	13/07/2020	31/05/2024
53	Tây Ninh	08/07/2020	31/05/2024
54	Thái Bình	25/06/2020	31/05/2024
55	**Thái Nguyên**	**19/11/2020**	**19/04/2024**
56	Thanh Hóa	29/09/2020	05/05/2024
57	Thừa Thiên Huế	29/07/2020	31/05/2024
58	Tiền Giang	24/09/2020	31/05/2024

59	Trà Vinh	29/07/2020	31/05/2024
60	Tuyên Quang	19/11/2020	20/05/2024
61	Vĩnh Long	25/06/2020	31/05/2024
62	**Vĩnh Phúc**	**30/06/2020**	**23/04/2024**
63	Yên Bái	26/08/2020	31/05/2024

Phụ lục VI
TÌNH HÌNH TRIỂN KHAI GIẢI PHÁP PHÒNG CHỐNG MÃ ĐỘC ĐÁP ỨNG YÊU CẦU CỦA CHỈ THỊ SỐ 14/CT-TTG NĂM 2018

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

1. Danh sách Bộ/Ngành

TT	Bộ/Cơ quan ngang Bộ/ Cơ quan trực thuộc Chính phủ	Số lượng máy chia sẻ dữ liệu trong tháng 05/2024	Ghi chú
1	Bộ Công Thương	63	
2	**Bộ Giáo dục và Đào tạo**	**0**	**Chưa chia sẻ**
3	Bộ Giao thông vận tải	86	
4	Bộ Kế hoạch và Đầu tư	1078	
5	Bộ Khoa học và Công nghệ	345	
6	**Bộ Lao động - Thương Binh và Xã hội**	**0**	**Mất kết nối 01 tháng trở lên**
7	Bộ Ngoại giao	9	
8	Bộ Nội vụ	411	
9	**Bộ Nông nghiệp và Phát triển nông thôn**	**0**	**Chưa chia sẻ**
10	Bộ Tài chính	262	
11	Bộ Tài nguyên và Môi trường	56	
12	Bộ Thông tin và Truyền thông	229	
13	Bộ Tư pháp	9997	
14	Bộ Văn hóa, Thể thao và Du lịch	22	
15	Bộ Xây Dựng	27	
16	Bộ Y tế	59	

17	Ngân hàng Nhà nước Việt Nam	1133	
18	**Thanh tra Chính phủ**	**0**	**Mất kết nối 01 tháng trở lên**
19	**Ủy ban Dân tộc**	**0**	**Chưa chia sẻ**
20	**Văn phòng Chính phủ**	**0**	**Mất kết nối 01 tháng trở lên**
21	Ban Quản lý Lăng Chủ tịch Hồ Chí Minh	4	
22	Bảo Hiểm Xã Hội	725	
23	Đài tiếng nói Việt Nam	12	
24	Đài Truyền hình Việt Nam	185	
25	Thông tấn xã Việt Nam	1629	
26	Viện Hàn Lâm KHCN	141	
27	Viện Hàn Lâm KHXH	196	
28	Kiểm toán Nhà nước Việt Nam	513	

2. Danh sách Tỉnh/Thành

TT	Tỉnh/Thành	Số lượng máy chia sẻ dữ liệu trong tháng 05/2024	Ghi chú
1	An Giang	480	
2	Bắc Giang	224	
3	Bắc Kạn	81	
4	Bạc Liêu	1880	
5	Bắc Ninh	162	
6	Bà Rịa - Vũng Tàu	44954	
7	Bến Tre	37	
8	Bình Định	68	
9	Bình Dương	10177	
10	Bình Phước	3795	
11	Bình Thuận	3253	
12	Cà Mau	3574	
13	Cần Thơ	1521	
14	Cao Bằng	9	
15	Đắk Lắk	84	
16	Đắk Nông	1161	

17	Đà Nẵng	29430	
18	Điện Biên	4195	
19	Đồng Nai	4152	
20	Đồng Tháp	8986	
21	Gia Lai	7	
22	Hà Giang	14	
23	Hải Dương	4573	
24	Hải Phòng	6	
25	Hà Nam	122	
26	Hà Nội	6239	
27	Hà Tĩnh	4237	
28	Hòa Bình	1038	
29	Hồ Chí Minh	9955	
30	Hậu Giang	975	
31	Hưng Yên	566	
32	Khánh Hòa	9	
33	Kiên Giang	2613	
34	Kon Tum	4841	

35	Lai Châu	35	
36	Lâm Đồng	2565	
37	Lạng Sơn	333	
38	Lào Cai	3	
39	Long An	2690	
40	Nam Định	38	
41	Nghệ An	1629	
42	Ninh Bình	16	
43	Ninh Thuận	905	
44	Phú Thọ	**0**	**Mất kết nối 01 tháng trở lên**
45	Phú Yên	98	
46	Quảng Bình	986	
47	Quảng Nam	134	
48	Quảng Ngãi	24	
49	**Quảng Ninh**	**0**	**Mất kết nối 01 tháng trở lên**
50	Quảng Trị	312	
51	Sóc Trăng	38	
52	Sơn La	7	

53	Tây Ninh	1385	
54	Thái Bình	3712	
55	Thái Nguyên	2020	
56	Thanh Hóa	1160	
57	Thừa Thiên Huế	1843	
58	Tiền Giang	4	
59	Trà Vinh	1261	
60	Tuyên Quang	**0**	**Mất kết nối 01 tháng trở lên**
61	Vĩnh Long	202	
62	Vĩnh Phúc	12757	
63	Yên Bái	1058	

Ghi chú:

- Số lượng máy của mỗi đơn vị được tính dựa trên số lượng máy chia sẻ thông tin về hệ điều hành (trường "OS" trong văn bản 2290/BTTTT-CATTT ngày 17/7/2018 về việc hướng dẫn kết nối, chia sẻ thông tin về mã độc giữa các hệ thống kỹ thuật phát hành).