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: 14 /BC-CATTT

Hà Nội, ngày 10 tháng 09 năm 2024

BÁO CÁO AN TOÀN THÔNG TIN MẠNG VIỆT NAM
(Tháng 8/2024)

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 **8/2024**, 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 **8/2024**, 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 25/9/2024.**

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

Văn bản số 1667/CATTT-NCSC về việc lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 8/2024 phát hành ngày 19/8/2024.

Văn bản số 1578/CATTT-NCSC về việc nhóm APT StormBamboo khai thác ISP để thực hiện tấn công diện rộng phát hành ngày 09/8/2024.

Văn bản số 1720/CATTT-NCSC về việc cảnh báo chiến dịch tấn công mạng có chủ đích nhằm tới Việt Nam phát hành ngày 29/8/2024.

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 **8/2024** đã có **87 đơn vị (63 Tỉnh/Thành, 24 Bộ/Ngành)** triển khai công tác giám sát an toàn thông tin và thực hiện kết nối chia sẻ dữ liệu giám sát với Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC). Thông qua kết nối chia sẻ dữ liệu giám sát từ **87 đơn vị**, Hệ thống kỹ thuật của Trung tâm Giám sát an toàn không gian mạng quốc gia ghi nhận **75/87** đơn vị có kết nối chia sẻ dữ liệu tương đối đầy đủ, **12/87** đơn vị không nhận được dữ liệu chia sẻ.

Theo ghi nhận từ Hệ thống kỹ thuật của Trung tâm Giám sát an toàn không gian mạng quốc gia cho thấy còn tồn tại nhiều đơn vị Bộ/Ngành, địa phương chưa thực hiện chia sẻ dữ liệu. Để đảm bảo an toàn thông tin mạng một cách đầy đủ và liên tục đối với các hệ thống, 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 **8/2024** đã có **88 đơn vị (63 Tỉnh/Thành, 25 Bộ/Ngành)** triển khai giải pháp phòng chống mã độc tập trung và thực hiện kết nối chia sẻ thông tin về mã độc với Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC). Hiện nay, còn tồn tại 03 đơn vị bao gồm: **Bộ Giáo dục và Đào tạo, Bộ Nông nghiệp và Phát triển nông thôn, Ủy ban Dân tộc** chưa thực hiện chia sẻ dữ liệu mã độc về Hệ thống kỹ thuật của Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC). Vì vậy, đề nghị các đơn vị thực hiện chia sẻ đầy đủ thông tin dữ liệu mã độc nhằm nâng cao năng lực phòng, chống phần mềm độc hại và thực hiện đánh giá chỉ số lây nhiễm phần mềm độc hại ở các bộ, ngành, địa phương, coi đây là một trong những tiêu chí đánh giá mức độ bảo đảm an toàn thông tin của các bộ, ngành, địa phương.

Thông qua việc kết nối chia sẻ dữ liệu về mã độc từ 88 đơn vị, Hệ thống kỹ thuật của Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC) ghi nhận **79/88 đơn vị** có kết nối thường xuyên. Trong các đơn vị kết nối thường xuyên có **79/79 đơn vị** chia sẻ về hệ điều hành các máy **(tổng số máy là 328.123)**.

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

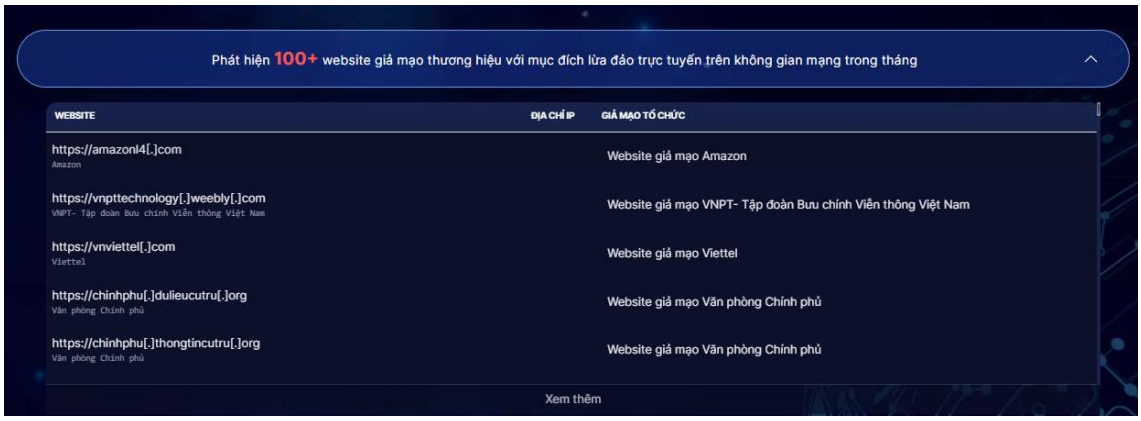
3. Phát hiện và ngăn chặn lừa đảo trên không gian mạng

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 **125.226 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 **8/2024**, hệ thống của NCSC đã phát hiện **55 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 **49.589** 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 **8/2024**, 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 8/2024:

TT	Mã điểm yếu/lỗ hổng	Mô tả	Ghi chú
1	CVE-2024-23897	- Điểm CVSS: 9.8 (Nghiêm trọng) - Mô tả: Lỗ hổng cho phép đối tượng tấn công truy cập và thực hiện các hành vi trái phép. - Ảnh hưởng: Jenkins - Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.	https://nvd.nist.gov/vuln/detail/CVE-2024-23897
2	CVE-2023-45249	- Điểm CVSS: 9.8 (Nghiêm trọng) - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã từ xa - Ảnh hưởng: Acronis Cyber Infrastructure - Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.	https://nvd.nist.gov/vuln/detail/CVE-2023-45249
3	CVE-2024-39717	- Điểm CVSS: 7.2 (Cao) - Mô tả: Lỗ hổng cho phép đối tượng tấn công truy cập và thực thi các hành vi trái phép. - Ảnh hưởng: Versa Director GUI	https://nvd.nist.gov/vuln/detail/CVE-2024-39717

		- Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.	
4	CVE-2024-6800	- Điểm CVSS: N/A - Mô tả: Lỗ hổng cho phép đối tượng tấn công truy cập và thực thi các hành vi trái phép. - Ảnh hưởng: GitHub Enterprise Server - Lỗ hổng chưa có mã khai thác và chưa bị khai thác trong thực tế.	https://nvd.nist.gov/vuln/detail/CVE-2024-6800
5	CVE-2024-7589	- Điểm CVSS: 8.1 (Cao) - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: FreeBSD - Lỗ hổng chưa có mã khai thác và đang bị khai thác trong thực tế.	https://nvd.nist.gov/vuln/detail/CVE-2024-7589
6	CVE-2024-7593	- Điểm CVSS: 9.8 (Nghiêm trọng) - Mô tả: Lỗ hổng cho phép đối tượng tấn công truy cập và thực hiện các hành vi trái phép - Ảnh hưởng: Ivanti vTM - Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.	https://nvd.nist.gov/vuln/detail/ CVE-2024-7593
7	CVE-2024-28000	- Điểm CVSS: 9.8 (Nghiêm trọng) - Mô tả: Lỗ hổng cho phép đối tượng tấn công leo thang đặc quyền. - Ảnh hưởng: LiteSpeed Technologies LiteSpeed Cache - Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.	https://nvd.nist.gov/vuln/detail/CVE-2024-28000
8	CVE-2024-37085	- Điểm CVSS: 7.2 (Cao) - Mô tả: Lỗ hổng cho phép đối tượng tấn công truy cập và thực hiện 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

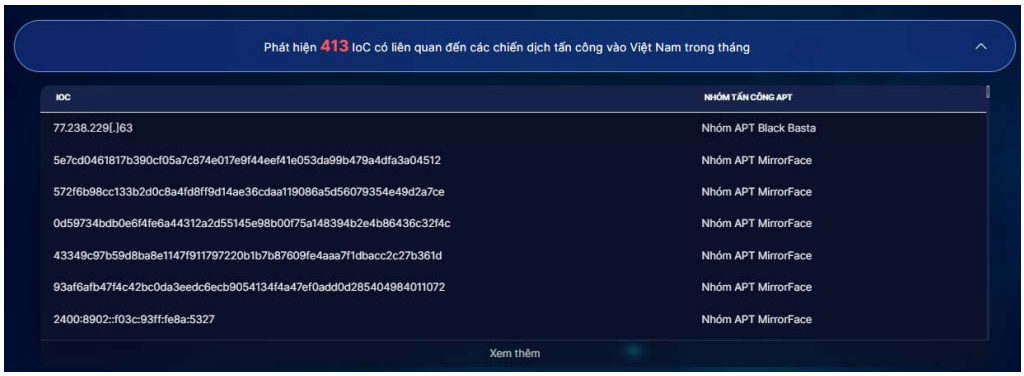
9	CVE-2024-38077	- Điểm CVSS: 9.8 (Nghiêm trọng) - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Windows Server 2008, Windows Server 2019, Windows Server 2012, Windows Server 2022, Windows Server 2016. - Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.	https://nvd.nist.gov/vuln/detail/CVE-2024-38077
10	CVE-2024-38063	- Điểm CVSS: 9.8 (Nghiêm trọng) - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Windows 10 - Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.	https://nvd.nist.gov/vuln/detail/CVE-2024-38063
11	CVE-2024-6387	- Điểm CVSS: 8.1 (Cao) - Mô tả: Lỗ hổng cho phép đối tượng tấn công truy cập và thực hiện 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
12	CVE-2024-40766	- Điểm CVSS: N/A - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ, truy cập và thực hiện các hành vi trái phép. - Ảnh hưởng: SonicWall SonicOS - Lỗ hổng chưa có mã khai thác và đang bị khai thác trong thực tế.	https://nvd.nist.gov/vuln/detail/CVE-2024-40766

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) đã phát hiện một số chiến dịch tấn công có chủ đích nhắm vào các tổ chức, doanh nghiệp, đơn vị tại Việt Nam. Cục An toàn thông tin đã phát hành Công văn số 1667/CATTT-NCSC ngày 19/8/2024 về việc lỗ hổng an toàn thông tin ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 08/2024; Công văn số 1578/CATTT-NCSC ngày 08/8/2024 về việc nhóm APT StormBamboo khai thác ISP để thực

hiện tấn công diện rộng; Công văn số 1720/CATTT-NCSC ngày 26/8/2024 về việc cảnh báo chiến dịch tấn công mạng có chủ đích nhằm tới Việt Nam.

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 **8/2024**, Trung tâm NCSC phát hiện **21 hệ thống** của các đơn vị có kết nối đến hạ tầng botnet. Trung tâm NCSC đã thực hiện chia sẻ các thông tin botnet này đến các đơn vị thông qua hệ thống phát hiện cảnh báo sớm botnet.

Thông tin các hệ thống ghi nhận nhiễm botnet trên hệ thống phát hiện cảnh báo sớm.

Ghi chú: *Danh sách các đơn vị có địa chỉ IP nằm trong botnet ghi nhận tại Phụ lục IV kèm theo.*

Đề nghị các đơn vị, tổ chức, doanh nghiệp nghiên cứu các thông tin về các nguy cơ rủi ro trong báo cáo, thực hiện rà soát hệ thống, xử lý các vấn đề về an toàn thông tin mạng trong hệ thống. Trong quá trình thực hiện, nếu có thông tin cần hỗ trợ đề nghị liên hệ với Trung tâm Giám sát an toàn không gian mạng quốc gia, Cục An toàn thông tin, Bộ Thông tin và Truyền thông, điện thoại: 024.3209.1616 hoặc số điện thoại trực đường dây nóng hỗ trợ giám sát, cảnh báo sớm 0961.405.333, thư điện tử: ncsc@ais.gov.vn./.

Nơi nhận:
- Thứ trưởng Phạm Đức Long (để b/c);
- Đơn vị chuyên trách về ATTT/CNTT của: Văn phòng Trung ương Đảng, Văn phòng Quốc hội, Văn phòng Chủ tịch nước, Tòa án Nhân dân tối cao, Viện Kiểm sát nhân dân tối cao, Kiểm toán Nhà nước;
- Đơn vị chuyên trách về ATTT/CNTT của các bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ;
- Sở TT&TT các tỉnh, thành phố trực thuộc TW;
- Các Tập đoàn kinh tế và Tổng công ty nhà nước;
- Các Tổ chức tài chính, Ngân hàng thương mại nhà nước; Các công ty Cổ phần Chứng khoán;
- 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 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;
- 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://amazonl4[.]com	Website giả mạo Amazon
2	https://vssid[.]pddgov[.]cc	Website giả mạo Bảo hiểm Xã hội Việt Nam
3	https://www[.]govn[.]cc	Website giả mạo Bộ Công An
4	https://ggiao[.]hangtietkiem[.]com	Website giả mạo Công ty cổ phần giao hàng tiết kiệm
5	https://www[.]giaohangtietkiem247[.]com	Website giả mạo Công ty cổ phần giao hàng tiết kiệm
6	https://www[.]cct-giaohangtietkiem[.]com	Website giả mạo Công ty cổ phần giao hàng tiết kiệm
7	https://dichvu[.]congtygiaohangtietkiemvn[.]com	Website giả mạo Công ty cổ phần giao hàng tiết kiệm
8	https://giaohangtietkiemvn[.]com	Website giả mạo Công ty cổ phần giao hàng tiết kiệm
9	https://nhanvienghtk[.]com	Website giả mạo Công ty cổ phần giao hàng tiết kiệm
10	https://vn[.]congtygiaohangtietkiemvn[.]com	Website giả mạo Công ty cổ phần giao hàng tiết kiệm
11	https://giaohangtietkiem247[.]top	Website giả mạo Công ty cổ phần giao hàng tiết kiệm
12	https://www[.]dautuphattrienvnfic[.]com	Website giả mạo Công ty Tài chính TNHH MTV Home Credit Việt Nam
13	https://dienmayxanh389[.]com	Website giả mạo Điện máy xanh

14	https://kbthuhoivontreo[.]com	Website giả mạo Kho bạc Nhà nước
15	https://acb[.]chamsocthekhachhang-tructuyen-thang8[.]com[.]vn	Website giả mạo Ngân hàng TMCP Á Châu
16	https://acb[.]chamsockhachhang-uudaithetructuyen-thang8[.]online	Website giả mạo Ngân hàng TMCP Á Châu
17	https://baovietn[.]vip	Website giả mạo Ngân hàng TMCP Bảo Việt
18	https://www[.]baovietvay[.]top	Website giả mạo Ngân hàng TMCP Bảo Việt
19	https://www[.]baovietin[.]top	Website giả mạo Ngân hàng TMCP Bảo Việt
20	https://www[.]baovietvc[.]top	Website giả mạo Ngân hàng TMCP Bảo Việt
21	https://ocb[.]hotrokhachhang-tructuyenthe[.]com	Website giả mạo Ngân hàng TMCP Phương Đông
22	https://vnsehotro[.]com	Website giả mạo Ngân hàng TMCP Quân đội
23	https://mbbkh-canhan[.]com	Website giả mạo Ngân hàng TMCP Quân đội
24	https://mmbonline01[.]com	Website giả mạo Ngân hàng TMCP Quân đội
25	https://hotro0nline28[.]com	Website giả mạo Ngân hàng TMCP Quân đội
26	https://vib[.]cham-soc-the-truc-tuyen[.]com[.]vn	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
27	https://lazada68[.]com	Website giả mạo sàn TMĐT Lazada
28	https://hethongnoibo[.]bio[.]link	Website giả mạo sàn TMĐT Lazada
29	https://hethongnoibo[.]bio[.]link	Website giả mạo sàn TMĐT Lazada

30	https://taichinheximbak[.]com	Website giả mạo sàn TMĐT Ngân Hàng TMCP Xuất Nhập Khẩu Việt Nam
31	https://sendotv[.]shop	Website giả mạo sàn TMĐT Sendo
32	https://www[.]vnsendotv[.]vip	Website giả mạo sàn TMĐT Sendo
33	https://sendovn[.]shop	Website giả mạo sàn TMĐT Sendo
34	https://www[.]shopeesopp[.]com	Website giả mạo sàn TMĐT Shopee
35	https://nuk36952s[.]com	Website giả mạo sàn TMĐT Shopee
36	https://sp61889p[.]com	Website giả mạo sàn TMĐT Shopee
37	https://558-558-559[.]com	Website giả mạo sàn TMĐT Shopee
38	nzx65821s[.]com	Website giả mạo sàn TMĐT Shopee
39	https://kpd63519s[.]com	Website giả mạo sàn TMĐT Shopee
40	https://tdke03[.]com	Website giả mạo sàn TMĐT Tiki
41	https://kyaj11[.]com	Website giả mạo sàn TMĐT Tiki
42	https://tikinew[.]club	Website giả mạo sàn TMĐT Tiki
43	https://tikijaj3[.]com	Website giả mạo sàn TMĐT Tiki
44	https://tikicareers[.]vip	Website giả mạo sàn TMĐT Tiki
45	https://sdfsshop1[.]com	Website giả mạo sàn TMĐT Tiki

46	https://www[.]tikivn84[.]com	Website giả mạo sàn TMĐT Tiki
47	https://tikimuasam24h[.]com	Website giả mạo sàn TMĐT Tiki
48	https://sjfku11[.]com	Website giả mạo sàn TMĐT Tiki
49	https://hethongtikicareers24h[.]com	Website giả mạo sàn TMĐT Tiki
50	https://hethongtikicareers24[.]com	Website giả mạo sàn TMĐT Tiki
51	https://sjfku88[.]com	Website giả mạo sàn TMĐT Tiki
52	https://chinhphu[.]thongtincutru[.]org	Website giả mạo Văn phòng Chính phủ
53	https://chinhphu[.]dulieucutru[.]org	Website giả mạo Văn phòng Chính phủ
54	https://vnviettel[.]com	Website giả mạo Viettel
55	https://vnpttechnology[.]weebly[.]com	Website giả mạo VNPT- Tập đoàn Bưu chính Viễn thông Việt Nam

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	15468	https://nvd.nist.gov/vuln/detail/ CVE-2022-26809
2	CVE-2023-21716	6697	https://nvd.nist.gov/vuln/detail/ CVE-2023-21716
3	CVE-2024-8035	5324	https://nvd.nist.gov/vuln/detail/ CVE-2023-8035
4	CVE-2024-8198	2334	https://nvd.nist.gov/vuln/detail/ CVE-2021-8198
5	CVE-2024-38223	2050	https://nvd.nist.gov/vuln/detail/ CVE-2024-38223
6	CVE-2024-7256	1844	https://nvd.nist.gov/vuln/detail/ CVE-2024-7256
7	CVE-2024-7550	1631	https://nvd.nist.gov/vuln/detail/ CVE-2021-7550
8	CVE-2024-7531	1595	https://nvd.nist.gov/vuln/detail/ CVE-2023-7531
9	CVE-2021-40444	992	https://nvd.nist.gov/vuln/detail/ CVE-2024-40444
10	CVE-2021-28310	781	https://nvd.nist.gov/vuln/detail/ CVE-2020-28310

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	harthat-api-v1.3.1.zip	Nhóm APT Moonstone Sleet
2	harthat-hash-v1.3.3.zip	
3	142.111.77[.]196	
4	d2a74db6b9c900ad29a81432af72eee8ed4e22bf61055e7e8f7a5f1a33778277	
5	spamicrosoft[.]com	Nhóm APT Black Basta
6	37.221.126[.]202	
7	91.196.70[.]160	
8	halagifts[.]com	
9	217.15.175[.]191	
10	preservedmoment[.]com	
11	45.155.249[.]97	
12	77.238.224[.]56	
13	77.238.229[.]63	
14	77.238.250[.]123	
15	77.238.245[.]233	
16	91.142.74[.]28	

17	191.142.74[.]28	
18	195.2.70[.]38	
19	falseaudiencekd[.]shop	
20	feighminoritsjda[.]shop	
21	justifycanddidatewd[.]shop	
22	marathonbeedksow[.]shop	
23	pleasurenarrowsdla[.]shop	
24	raiseboltskdlwpow[.]shop	
25	richardflorespoew[.]shop	
26	strwawrunnygjwu[.]shop	
27	167[.]88[.]173[.]173	Mã độc Trojan MoonPeak
28	80[.]71[.]157[.]55	
29	45[.]87[.]153[.]79	
30	104[.]194[.]152[.]251	
31	pumaria[.]store	
32	212[.]224[.]107[.]244	
33	nmailhostserver[.]store	
34	91[.]194[.]161[.]109	
35	95[.]164[.]86[.]148	

36	84[.]247[.]179[.]77	
37	45[.]95[.]11[.]52	
38	yoiroyse[.]store	
39	27[.]255[.]81[.]118	
40	27[.]255[.]80[.]162	
41	210[.]92[.]18[.]169	
42	nsonlines[.]store	
43	msn-microsoft[.] org	Nhóm APT41; mã độc CobaltStrike
44	s3bucket-azure[.] online	
45	s3-microsoft[.] com	
46	visualstudio-microsoft[.] com	
47	krislab[.] site	
48	s2cloud-amazon[.] com	
49	s3cloud-azure[.] com	
50	trendmicrotech[.] com	
51	xtools[.] lol	
52	45[.]66[.]217[.]106	Nhóm APT MirrorFace
53	45[.]77[.]12[.]212	
54	207[.]148[.]97[.]235	

55	64[.]176[.]214[.]51	
56	45[.]76[.]222[.]130	
57	207[.]148[.]90[.]45	
58	103[.]143[.]208[.]115	
59	103[.]143[.]209[.]36	
60	91[.]245[.]255[.]30	
61	www[.]lookpumrron[.]com	
62	minggamevies[.]com	
63	89[.]233[.]109[.]69	
64	108[.]160[.]130[.]45	
65	95[.]85[.]91[.]15	
66	168[.]100[.]8[.]103	
67	45[.]77[.]183[.]161	Nhóm APT MirrorFace
68	207[.]148[.]103[.]42	
69	103[.]143[.]208[.]29	
70	146[.]70[.]79[.]68	
71	91[.]245[.]255[.]79	
72	www[.]morrowadded[.]com	
73	2001:19f0:7001:2ae2:5400:4ff:fe0a:5566	

74	2a12:a300:3700::5d9f:b451	
75	bcd34d436cbac235b56ee5b7273baed62bf385ee13721c7fdcfc00af9ed63997	
76	4f932d6e21fdd0072aba61203c7319693e490adbd9e93a49b0fe870d4d0aed71	
77	9590646b32fec3aafd6c648f69ca9857fb4be2adfabf3bcaf321c8cd25ba7b83	
78	7a7e7e0d817042e54129697947dfb423b607692f4457163b5c62ffea69a8108d	
79	b07c7dfb3617cd40edc1ab309a68489a3aa4aa1e8fd486d047c155c952dc509e	
80	2a12:a300:3600::31b5:2e02	
81	2400:8902::f03c:93ff:fe8a:5327	
82	93af6afb47f4c42bc0da3eedc6ecb9054134f4a47ef0add0d285404984011072	
83	43349c97b59d8ba8e1147f911797220b1b7b87609fe4aaa7f1dbacc2c27b361d	
84	0d59734bdb0e6f4fe6a44312a2d55145e98b00f75a148394b2e4b86436c32f4c	
85	572f6b98cc133b2d0c8a4fd8ff9d14ae36cdaa119086a5d56079354e49d2a7ce	
86	5e7cd0461817b390cf05a7c874e017e9f44eef41e053da99b479a4dfa3a04512	

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 07/2024	Số lượng IP botnet tháng 08/2024	Loại mã độc/botnet
1	Bộ Khoa học và Công nghệ	0	2	Andromeda
2	Bảo hiểm Xã hội Việt Nam	1	1	Andromeda
3	Đài Tiếng nói Việt Nam	1	1	Andromeda

2. Danh sách Tỉnh/thành

STT	Tên đơn vị	Số lượng IP botnet tháng 07/2024	Số lượng IP botnet tháng 08/2024	Ghi chú
1	Lai Châu	2	6	Andromeda
2	Hà Nam	5	5	Andromeda
3	Thanh Hóa	2	4	Andromeda
4	Điện Biên	2	3	Andromeda
5	Lâm Đồng	3	3	Andromeda
6	Thái Bình	2	2	Andromeda
7	An Giang	1	1	Andromeda
8	Bà Rịa Vũng Tàu	1	1	Andromeda
9	Cao Bằng	1	1	Andromeda

10	Gia Lai	1	1	Andromeda
11	Hà Nội	1	1	Andromeda
12	Kon Tum	1	1	Andromeda
13	Lạng Sơn	2	1	Andromeda
14	Nam Định	2	1	Andromeda
15	Ninh Bình	2	1	Andromeda
16	Quảng Ninh	1	1	Andromeda
17	Lào Cai	0	1	Andromeda
18	Quảng Trị	0	1	Andromeda
19	Đắk Nông	1	0	Andromeda