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: 16 /BC-CATTT

Hà Nội, ngày 08 tháng 10 năm 2024

BÁO CÁO AN TOÀN THÔNG TIN MẠNG VIỆT NAM
(Tháng 9/2024)

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.

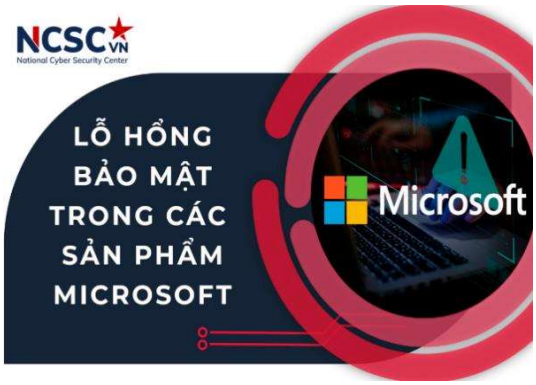
Báo cáo cung cấp thông tin về các sự kiện an toàn thông tin mạng, xu hướng tấn công mạng, các lỗ hổng an toàn thông tin mới được công bố… Thông tin này giúp các cơ quan, tổ chức nắm bắt kịp thời các vấn đề an toàn thông tin mạng đang diễn ra từ đó có thể chủ động triển khai kịp thời các biện pháp (con người, quy trình, công nghệ) để bảo đảm an toàn thông tin cho cơ quan, tổ chức mình.

Trong tháng **9/2024**, 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 **9/2024**, 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 25/10/2024.**

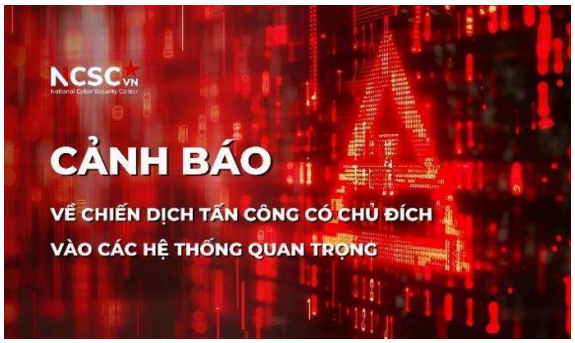
1. Cảnh báo an toàn thông tin đã phát hành trong tháng

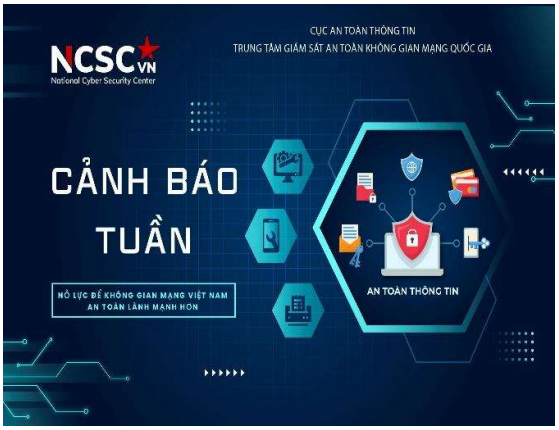


Báo cáo về các lỗ hổng an toàn thông tin trong các sản phẩm của Microsoft tháng 9/2024.

Thông tin chi tiết tại: https://khonggianmang.vn/alert/lo-hong-bao-mat-co-muc-anh-huong-cao-va-nghiem-trong-trong-cac-san-pham-microsoft-cong-bo-thang-09-2024.238

Văn bản số 1778/CATTT-NCSC về việc Cảnh báo về chiến dịch tấn công có chủ đích vào các hệ thống quan trọng phát hành ngày 11/9/2024.





Cảnh báo an toàn thông tin phát hành hàng tuần trên không gian mạng cung cấp thông tin kịp thời về các nguy cơ an toàn thông tin, lỗ hổng bảo mật và khuyến nghị kỹ thuật, giúp cơ quan và doanh nghiệp chủ động phòng ngừa và xử lý sự cố.

Thông tin chi tiết tại: https://khonggianmang.vn/

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 **9/2024** 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 **74/87** đơn vị có kết nối chia sẻ dữ liệu tương đối đầy đủ, **13/87** đơn vị không nhận được dữ liệu chia sẻ.

Theo ghi nhận từ Hệ thống kỹ thuật của Trung tâm Giám sát an toàn không gian mạng quốc gia cho thấy còn tồn tại nhiều đơn vị Bộ/Ngành, địa phương chưa thực hiện chia sẻ dữ liệu. Để đảm bảo an toàn hệ thống thông tin quốc gia, Cục An toàn thông tin đề nghị các đơn vị khẩn trương triển khai nghiêm túc và chặt chẽ các quy định theo chỉ thị của Thủ tướng Chính phủ để thực hiện việc chia sẻ dữ liệu nhằm đảm bảo tính liên thông, an toàn và hiệu quả trong quản lý và điều hành hệ thống thông tin quốc gia.

Ghi chú: *Danh sách tình trạng triển khai công tác giám sát của các đơn vị tại* ***Phụ lục V*** *kèm theo.*

Tình hình triển khai giải pháp phòng chống mã độc đáp ứng yêu cầu của Chỉ thị số 14/CT-TTG năm 2018. Đến tháng **9/2024** 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 **76/88 đơn vị** có kết nối thường xuyên. Trong các đơn vị kết nối thường xuyên có **76/76 đơn vị** chia sẻ về hệ điều hành các máy **(tổng số máy là 294.800)**.

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

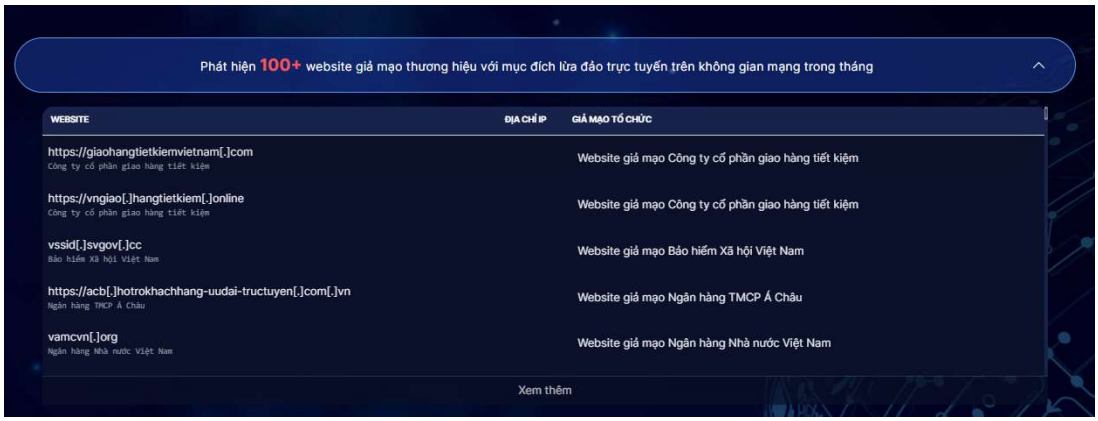
3. Phát hiện và ngăn chặn lừa đảo trên không gian mạng

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 **125.338 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 **9/2024**, hệ thống của NCSC đã phát hiện **31 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.*

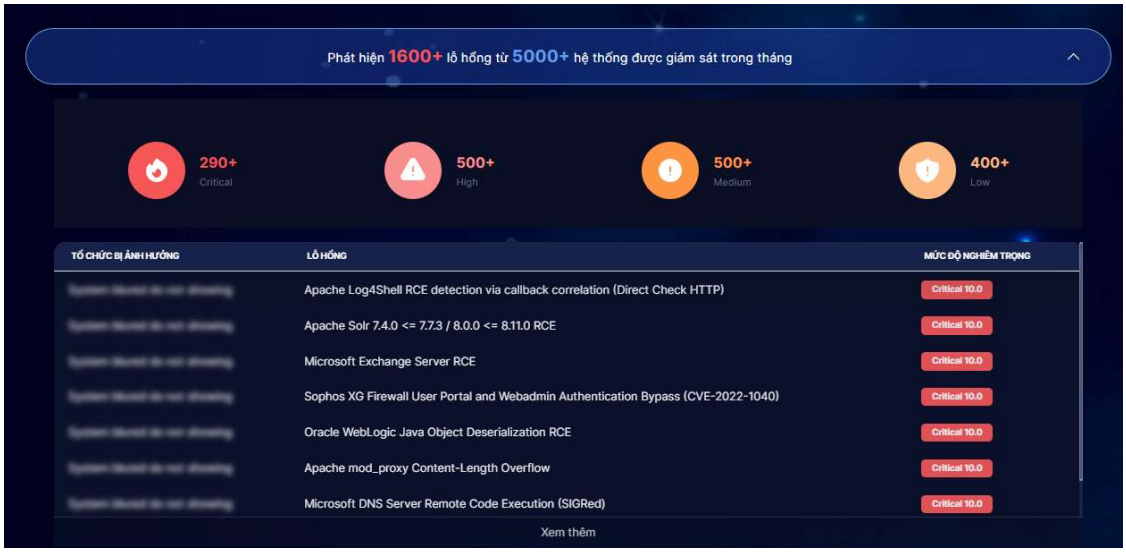
4. Phát hiện và cảnh báo sớm các lỗ hổng của các hệ thống thông tin trên không gian mạng

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 **45.691** 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 **9/2024**, 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 9/2024:

TT	Mã điểm yếu/lỗ hổng	Mô tả	Ghi chú
1	CVE-2024-40766	- Điểm CVSS: 9.8 (Nghiêm trọng) - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ. - Ảnh hưởng: SonicWall SonicOS. - Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.	https://nvd.nist.gov/vuln/detail/CVE-2024-40766
2	CVE-2024-29847	- Điểm CVSS: 9.8 (Nghiêm trọng) - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Ivanti EPM. - Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.	https://nvd.nist.gov/vuln/detail/CVE-2024-29847
3	CVE-2024-38812	- Điểm CVSS: 9.8 (Nghiêm trọng) - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: vCenter Server.	https://nvd.nist.gov/vuln/detail/CVE-2024-38812

		- Lỗ hổng chưa có mã khai thác và đang bị khai thác trong thực tế.	
4	CVE-2024-36401	- Điểm CVSS: 9.8 (Nghiêm trọng) - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: GeoServer. - Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.	https://nvd.nist.gov/vuln/detail/CVE-2024-36401
5	CVE-2024-7261	- Điểm CVSS: 9.8 (Nghiêm trọng) - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Zyxel firmware - Lỗ hổng chưa có mã khai thác và đang bị khai thác trong thực tế.	https://nvd.nist.gov/vuln/detail/CVE-2024-7261
6	CVE-2024-43461	- Điểm CVSS: 8.8 (Cao) - Mô tả: Lỗ hổng cho phép đối tượng tấn công truy cập và thực thi các hành vi trái phép. - Ảnh hưởng: Microsoft Windows 10, Windows 11, Windows Server 2008, 2012, 2016, 2019, 2022. - Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.	https://nvd.nist.gov/vuln/detail/CVE-2024-43461
7	CVE-2024-8190	- Điểm CVSS: 7.2 (Cao) - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Ivanti Cloud Services Appliance - Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.	https://nvd.nist.gov/vuln/detail/CVE-2024-8190
8	CVE-2024-6670	- Điểm CVSS: 9.8 (Nghiêm trọng) - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực hiện tấn công SQL Injection. - Ảnh hưởng: WhatsUp Gold. - Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.	https://nvd.nist.gov/vuln/detail/CVE-2024-6670

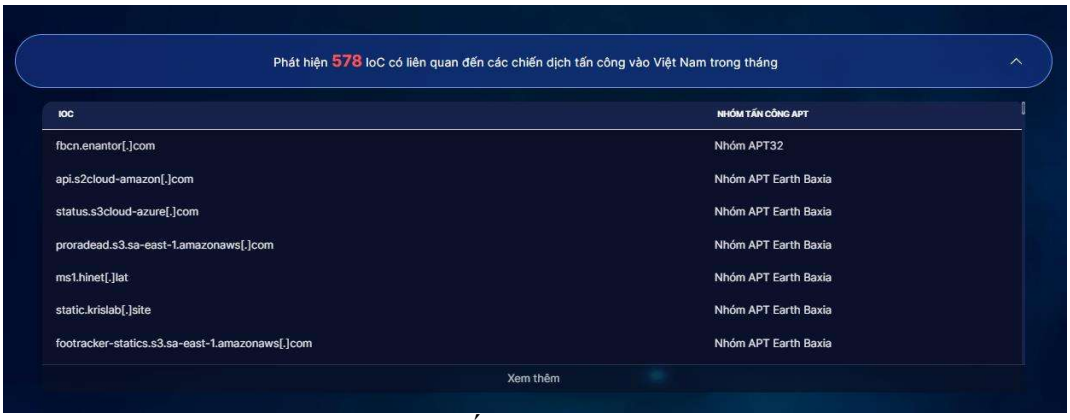
9	CVE-2024-6342	- Điểm CVSS: 9.8 (Nghiêm trọng) - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Zyxel firmware. - Lỗ hổng chưa có mã khai thác và đang bị khai thác trong thực tế.	https://nvd.nist.gov/vuln/detail/CVE-2024-6342
10	CVE-2024-38112	- Điểm CVSS: 7.5 (Cao) - Mô tả: Lỗ hổng cho phép đối tượng tấn công truy cập và thực thi các hành vi trái phép. - Ảnh hưởng: Microsoft Windows 10, Windows 11, Windows Server 2008, 2012, 2016, 2019, 2022. - Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.	https://nvd.nist.gov/vuln/detail/CVE-2024-38112
11	CVE-2024-37084	- Điểm CVSS: 8.8 (Cao) - Mô tả: Lỗ hổng cho phép đối tượng tấn công truy cập và thực thi các hành vi trái phép. - Ảnh hưởng: Spring Cloud Data Flow. - Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.	https://nvd.nist.gov/vuln/detail/CVE-2024-37084
12	CVE-2024-40711	- Điểm CVSS: 9.8 (Nghiêm trọng) - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Veeam. - Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.	https://nvd.nist.gov/vuln/detail/CVE-2024-40711

5. Phân tích rủi ro và cảnh báo sớm các nguy cơ tấn công có chủ đích

Thực hiện phân tích, theo dõi và dự báo, cảnh báo sớm xu hướng về tấn công mạng, Cục An toàn thông tin (Bộ Thông tin và Truyền thông) phát hiện xu hướng tấn công mã hóa tống tiền (ransomware) tăng cao trong thời gian gần đây. Đã có một số hệ thống thông tin của cơ quan, tổ chức, doanh nghiệp tại Việt Nam bị sự cố tấn công, gây gián đoạn hoạt động và thiệt hại về vật chất, hình ảnh của các cơ quan, tổ chức, doanh nghiệp, cũng như hoạt động bảo đảm an toàn không gian mạng quốc gia. Cục An toàn thông tin đã phát hành Công văn số 1778/CATTT-

NCSC về việc Cảnh báo về chiến dịch tấn công có chủ đích vào các hệ thống quan trọng phát hành ngày 11/09/2024.

Trung tâm NCSC đã tiến hành thu thập, phân tích và phát hiện nhiều chỉ báo (Indicators of compromise) về tấn công mạng có thể ảnh hưởng đến cơ quan, tổ chức, doanh nghiệp Việt Nam. Các đơn vị cần chủ động rà soát các máy chủ, máy trạm, rà soát toàn bộ các hệ thống giám sát theo các chỉ báo mà Trung tâm NCSC cung cấp trong báo cáo nhằm xử lý sớm các rủi ro trong hệ thống, liên tục cập nhật các chỉ báo về tấn công mạng, đặc biệt là các chỉ báo đã được chia sẻ từ hệ thống của Trung tâm NCSC.



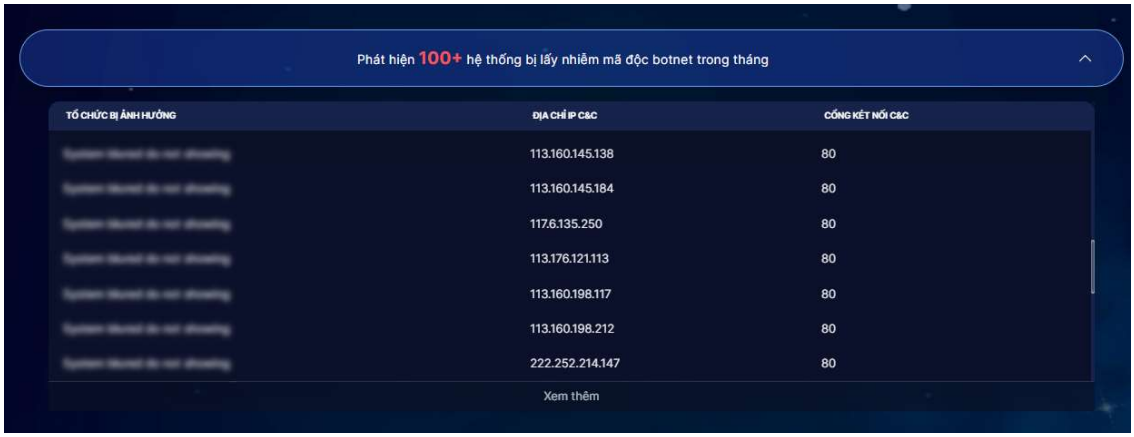
Thông tin IOC được cung cấp tại https://alert.khonggianmang.vn/

Ghi chú: *Danh sách các IOC có thể ảnh hưởng tới cơ quan, tổ chức doanh nghiệp Việt Nam ghi nhận tại Phụ lục III kèm theo.*

6. Phát hiện và cảnh báo sớm các nguy cơ botnet trong hệ thống

Thực hiện việc phân tích và phát hiện sớm các nguy cơ từ bên trong hệ thống, đặc biệt là các nguy cơ máy chủ, máy trạm trong hệ thống nhiễm mã độc, trở thành botnet. Hệ thống giám sát của NCSC đã thực hiện thu thập chia sẻ thông tin về các mối đe dọa trên không gian mạng với các tổ chức quốc tế, giám sát liên tục các mạng lưới botnet.

Trong tháng **9/2024**, Trung tâm NCSC phát hiện **18 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;
- 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;
- Các doanh nghiệp: VNPOST, VTC;
- Cục trưởng;
- Phó Cục trưởng Trần Quang Hưng;
- Các phòng: ATHTTT, TT&HTQT;
- Trung tâm VNCERT/CC;
- Lưu: VT, NCSC.LTQ.

CỤC TRƯỞNG

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

Lê Văn Tuấn

Phụ lục I

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

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

TT	Website giả mạo	Ghi chú
1	vssid[.]svgov[.]cc	Website giả mạo Bảo hiểm Xã hội Việt Nam
2	https://giaohangtietkiem247[.]top	Website giả mạo Công ty cổ phần giao hàng tiết kiệm
3	https://vngiao[.]hangtietkiem[.]online	Website giả mạo Công ty cổ phần giao hàng tiết kiệm
4	https://giaohangtietkiemvietnam[.]com	Website giả mạo Công ty cổ phần giao hàng tiết kiệm
5	tongcongtygiaohangtietkiem[.]com	Website giả mạo Công ty cổ phần giao hàng tiết kiệm
6	vanchuyenghtka[.]com	Website giả mạo Công ty cổ phần giao hàng tiết kiệm
7	https://org[.]govqp[.]com	Website giả mạo Cục Đăng kiểm Việt Nam
8	dichvucong[.]bcavnvnvngov[.]com	Website giả mạo Dịch vụ công Quốc Gia
9	https://www[.]ebayu[.]top	Website giả mạo sàn TMĐT Ebay
10	https://github-scanner[.]com	Website giả mạo Github
11	https://play[.]appgoogle[.]cc	Website giả mạo Google
12	https://hethongnoibo[.]bio[.]link	Website giả mạo sàn TMĐT Lazada
13	thecaosieutoc[.]shop	Website giả mạo sàn TMĐT MoMo

14	vamcvn[.]org	Website giả mạo Ngân hàng Nhà nước Việt Nam
15	https://acb[.]hotrokhachhang-uudai-tructuyen[.]com[.]vn	Website giả mạo Ngân hàng TMCP Á Châu
16	https://acb[.]uudaikhachhangthe-tructuyen-thang9[.]com[.]vn	Website giả mạo Ngân hàng TMCP Á Châu
17	https://baovietcv[.]top	Website giả mạo Ngân hàng TMCP Bảo Việt
18	https://www[.]baovietvc[.]top	Website giả mạo Ngân hàng TMCP Bảo Việt
19	ocb[.]chamsocthekhachhang-uudai-tructuyen-thang9[.]com[.]vn	Website giả mạo Ngân hàng TMCP Phương Đông
20	https://mbdk555[.]com	Website giả mạo Ngân hàng TMCP Quân đội
21	https://tienichshiinhan[.]com	Website giả mạo Ngân hàng TNHH MTV Shinhan Việt Nam
22	https://www[.]lapmangsctv[.]com[.]vn	Website giả mạo SCTV
23	https://sendovn[.]shop	Website giả mạo sàn TMĐT Sendo
24	https://kpd63519s[.]com	Website giả mạo sàn TMĐT Shopee
25	https://kpt32165s[.]com	Website giả mạo sàn TMĐT Shopee
26	www[.]shopeeace[.]com	Website giả mạo sàn TMĐT Shopee
27	nzu66938s[.]com	Website giả mạo sàn TMĐT Shopee
28	https://muasamtiki24h[.]com	Website giả mạo sàn TMĐT Tiki
29	https://tiktikshopvn[.]com	Website giả mạo sàn TMĐT Tiki
30	https://chinhphu[.]hodancu[.]com	Website giả mạo Văn phòng Chính phủ

31	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	15013	https://nvd.nist.gov/vuln/detail/ CVE-2022-26809
2	CVE-2023-21716	6678	https://nvd.nist.gov/vuln/detail/ CVE-2023-21716
3	CVE-2024-43495	3541	https://nvd.nist.gov/vuln/detail/ CVE-2024-43495
4	CVE-2024-8362	2128	https://nvd.nist.gov/vuln/detail/ CVE-2024-8362
5	CVE-2024-8389	1921	https://nvd.nist.gov/vuln/detail/ CVE-2024-8389
6	CVE-2024-8198	1839	https://nvd.nist.gov/vuln/detail/ CVE-2024-8198
7	CVE-2021-40444	996	https://nvd.nist.gov/vuln/detail/ CVE-2021-40444
8	CVE-2024-9123	812	https://nvd.nist.gov/vuln/detail/ CVE-2024-9123
9	CVE-2024-8035	790	https://nvd.nist.gov/vuln/detail/ CVE-2024-8035
10	CVE-2021-28310	771	https://nvd.nist.gov/vuln/detail/ CVE-2021-28310

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	51.81.29[.]44	Nhóm **APT32**
2	5.230.35[.]192	
3	185.198.57[.]184	
4	46.183.223[.]79	
5	hx-in-f211[.]popfan[.]org	
6	185.43.220[.]188	
7	193.107.109[.]148	
8	176.103.63[.]48	
9	adobe[.]riceaub[.]com	
10	cds55[.]lax8[.]setalz[.]com	
11	fbcn.enantor[.]com	
12	priv[.]manuelleake[.]com	
13	blank[.]eatherurg[.]com	
14	cdn.arlialter[.]com	
15	fbcn.enantor[.]com	
16	ww1.erabend[.]com	

17	var.alieras[.]com	
18	2-can.njalla[.]in	
19	3-get.njalla[.]fo	
20	46.183.223[.]79	
21	var.alieras[.]com	
22	176.103.63[.]48	
23	185.198.57[.]184	
24	get.dupbleanalytics[.]net	
25	cdn.arlialter[.]com	
26	ww1.erabend[.]com	Nhóm **APT32**
27	cds55[.]lax8[.]setalz[.]com	
28	hx-in-f211[.]popfan[.]org	
29	adobe[.]riceaub[.]com	
30	blank[.]eatherurg[.]com	
31	priv[.]manuelleake[.]com	
32	base.msteamsapi[.]com	
33	kpi.adcconnect[.]me	
34	you.can-get-no[.]info	
35	1-you.njalla[.]no	

36	dupbleanalytics[.]net	
37	178.128.221.202:443	Chiến dịch tấn công **Crimson Palace**
38	192.142.18.27	
39	45.15.143.151	
40	cancelle.net	
41	103.56.5.224	
42	141.136.44.219	
43	66.42.56.233	
44	45.9.191.183	
45	191.96.53.132	
46	95.179.249.205	
47	gsenergyspeedtest.com	
48	192.142.18.25	
49	198.244.237.13	
50	dmsz.org	
51	49.157.28.114	
52	145.14.158.235	
53	test1.zhangliyong.cn	
54	www.pmshyptest.com	

55	45.77.46.245:443	
56	198.13.47.158:443	
57	192.142.18.15	
58	hpupdate.net	
59	123.253.35.100	
60	gandeste.net	
61	103.19.16.248:443	
62	107.148.41.114	
63	191.96.53.132: 443	
64	64.176.50.42:8444	
65	64.176.37.107:443	
66	128.199.107.213	
67	114[.]255[.]70[.]20	Nhóm APT **Flax Typhoon**
68	5[.]188[.]33[.]135	
69	202[.]182[.]109[.]151	
70	5[.]188[.]33[.]135	
71	5[.]188[.]33[.]228	
72	185[.]14[.]45[.]160	
73	185[.]207[.]154[.]253	

74	14[.]1[.]98[.]223	
75	223[.]98[.]159[.]112	
76	210[.]61[.]186[.]117	
77	104[.]244[.]89[.]157	
78	114[.]255[.]70[.]30	
79	195[.]234[.]62[.]188	
80	195[.]234[.]62[.]192	
81	85[.]90[.]216[.]69	
82	195[.]234[.]62[.]184	
83	89[.]44[.]198[.]200	
84	207[.]148[.]68[.]131	
85	108[.]61[.]177[.]81	
86	45[.]80[.]215[.]149	
87	45[.]92[.]70[.]111	
88	45[.]13[.]199[.]140	
89	abpi[.]b2047[.]com	
90	45[.]13[.]199[.]84	
91	45[.]13[.]199[.]96	
92	45[.]13[.]199[.]104	

93	45[.]13[.]199[.]45	
94	45[.]135[.]117[.]136	
95	45[.]10[.]58[.]133	
96	45[.]10[.]58[.]130	
97	85[.]90[.]216[.]111	
98	5[.]8[.]33[.]26	
99	45[.]10[.]58[.]128	
100	195[.]234[.]62[.]197	
101	45[.]92[.]70[.]68	
102	5[.]45[.]184[.]68	Nhóm APT **Flax Typhoon**
103	195[.]234[.]62[.]198	
104	92[.]38[.]185[.]47	
105	92[.]38[.]185[.]43	
106	85[.]90[.]216[.]112	
107	45[.]10[.]58[.]129	
108	5[.]181[.]27[.]219	
109	139[.]180[.]137[.]219	
110	149[.]248[.]51[.]22	
111	65[.]20[.]97[.]251	

112	iycwqot[.]com	
113	92[.]38[.]185[.]44	
114	45[.]135[.]117[.]131	
115	85[.]90[.]216[.]110	
116	37[.]61[.]229[.]17	
117	37[.]9[.]35[.]89	
118	85[.]90[.]216[.]116	
119	37[.]61[.]229[.]15	
120	92[.]38[.]185[.]46	
121	45[.]80[.]215[.]186	Nhóm APT **Flax Typhoon**
122	85[.]90[.]216[.]115	
123	45[.]10[.]58[.]132	
124	92[.]38[.]185[.]45	
125	45[.]92[.]70[.]71	
126	207[.]148[.]122[.]69	
127	91[.]216[.]190[.]154	
128	23[.]236[.]68[.]193	
129	91[.]216[.]190[.]247	
130	91[.]216[.]190[.]74	

131	45[.]80[.]215[.]47	
132	92[.]223[.]30[.]232	
133	92[.]223[.]30[.]241	
134	202[.]182[.]109[.]151	
135	mail[.]k3121[.]com	
136	45[.]80[.]215[.]155	
137	89[.]44[.]198[.]195	
138	45[.]80[.]215[.]152	
139	202[.]182[.]109[.]151	
140	89[.]44[.]198[.]254	Nhóm APT **Flax Typhoon**
141	91[.]216[.]190[.]2	
142	91[.]216[.]190[.]80	
143	23[.]236[.]68[.]213	
144	23[.]236[.]69[.]82	
145	23[.]236[.]68[.]161	
146	23[.]236[.]69[.]110	
147	23[.]236[.]68[.]229	
148	hy92[.]com	
149	hy830[.]com	

150	hy529[.]com	Nhóm APT **Flax Typhoon**
151	hy229[.]com	
152	hy324[.]com	
153	hy1025[.]com	
154	hy42[.]com	
155	hy619[.]com	
156	hy424[.]com	
157	hy811[.]com	
158	wmllxwkg[.]w8510[.]com	
159	ecvkiehs[.]com	
160	hfsdln[.]com	
161	osiso[.]com	
162	bcdkwwuah[.]com	
163	cvmnomvxm[.]com	
164	cvgeuwo[.]com	
165	lofeuq[.]com	
166	lznmihdej[.]com	
167	fajxtg[.]com	
168	grntjr[.]com	

169	oploz[.]com	
170	mudvw[.]com	
171	amdord[.]com	
172	mvxnspcqr[.]com	
173	adjsn[.]com	
174	ttcyci[.]com	
175	glxxet[.]com	
176	nmfagp[.]com	
177	rnjca[.]com	
178	woaba[.]com	
179	bxgtbv[.]com	
180	ykcmewapc[.]com	
181	obqlibg[.]com	
182	recordar-simmco.s3.sa-east-1.amazonaws[.]com	Nhóm APT **Earth Baxia**
183	wordpresss-data.s3.me-south-1.amazonaws[.]com	
184	ecgglass-arq.s3.sa-east-1.amazonaws[.]com	
185	souzacambos.s3.sa-east-1.amazonaws[.]com	
186	cooltours.s3.sa-east-1.amazonaws[.]com	
187	s3-contemp.s3.sa-east-1.amazonaws[.]com	

188	homologacao-sisp.s3.sa-east-1.amazonaws[.]com	
189	doare-assets.s3.sa-east-1.amazonaws[.]com	
190	kcalmoments.s3.me-south-1.amazonaws[.]com	
191	speedshare.oss-cn-hongkong.aliyuncs[.]com	
192	167.172.89[.]142	
193	167.172.84[.]142	
194	152.42.243[.]170	
195	188.166.252[.]85	
196	xiiltrionsoledadprod.s3.sa-east-1.amazonaws[.]com	
197	app-dimensiona.s3.sa-east-1.amazonaws[.]com	
198	bjj-files-production.s3.sa-east-1.amazonaws[.]com	
199	footracker-statics.s3.sa-east-1.amazonaws[.]com	
200	static.krislab[.]site	
201	ms1.hinet[.]lat	
202	proradead.s3.sa-east-1.amazonaws[.]com	
203	status.s3cloud-azure[.]com	
204	api.s2cloud-amazon[.]com	
205	visualstudio-microsoft[.]com	
206	us2.s3bucket-azure[.]online	

207	static.trendmicrotech[.]com	
208	msa.hinet[.]ink	
209	bobs8.oss-cn-hongkong.aliyuncs[.]com	
210	rocean.oca[.]pics	
211	360photo.oss-cn-hongkong.aliyuncs[.]com	

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 8/2024	Số lượng IP botnet tháng 9/2024	Loại mã độc/botnet
1	Bộ Khoa học và Công nghệ	2	2	Ranbyus; Matsnu; 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 8/2024	Số lượng IP botnet tháng 9/2024	Ghi chú
1	Lai Châu	6	5	Andromeda
2	Hà Nam	5	3	Andromeda
3	Thanh Hóa	4	2	Andromeda
4	Điện Biên	3	2	Andromeda
5	Thái Bình	2	2	Andromeda
6	Bà Rịa Vũng Tàu	1	2	Andromeda
7	Lâm Đồng	3	1	Andromeda
8	An Giang	1	1	Andromeda
9	Gia Lai	1	1	Andromeda

10	Hà Nội	1	1	Andromeda
11	Lạng Sơn	1	1	Andromeda
12	Nam Định	1	1	Andromeda
13	Ninh Bình	1	1	Andromeda
14	Quảng Ninh	1	1	Andromeda
15	Quảng Trị	1	1	Andromeda