

Số: /BC-CATTT

Hà Nội, ngày tháng năm 2024

**BÁO CÁO AN TOÀN THÔNG TIN MẠNG VIỆT NAM**  
**(Tháng 7/2024)**

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 7/2024, 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 7/2024, 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 25/8/2024**.

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



Văn bản số 1310/CATTT-NCSC về việc lỗ hổng bảo mật ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 07/2024 phát hành ngày 12/07/2024.

Trung tâm NCSC đã phát hành các tin cảnh báo hàng tuần trên <https://khonggianmang.vn/> về các vấn đề an toàn thông tin trên không gian mạng; ghi nhận, thống kê số liệu về tình trạng an toàn thông tin tại Việt Nam trong tháng vừa qua.



## 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 7/2024 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 **73/87** đơn vị có kết nối chia sẻ dữ liệu tương đối đầy đủ, **14/87** 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 7/2024 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 **82/88 đơn vị** có kết nối thường xuyên. Trong các đơn vị kết nối thường xuyên có **82/82 đơn vị** chia sẻ về hệ điều hành các máy (**tổng số máy là 274.557**).

***Ghi chú:*** Danh sách tình 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 **125.059 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 7/2024, hệ thống của NCSC đã phát hiện **125 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.



WEBSITE	ĐỊA CHỈ IP	GIẢ MẠO TỔ CHỨC
https://shop[.]global-selling[.]top TMDT Amazon		Website giả mạo sàn TMDT Amazon
https://lazadaevent[.]com TMDT Lazada		Website giả mạo sàn TMDT Lazada
https://zdkiemdon24[.]com TMDT Lazada		Website giả mạo sàn TMDT Lazada
https://da1215[.]com TMDT Lazada		Website giả mạo sàn TMDT Lazada
https://www[.]hethongnhanvien[.]com TMDT Lazada		Website giả mạo sàn TMDT Lazada

*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 **36.497** 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 7/2024, 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 7/2024:**

TT	Mã điểm yếu/lỗ hổng	Mô tả	Ghi chú
1	CVE-2024-6387	<ul style="list-style-type: none"> <li>- Điểm CVSS: 8.1 (Cao)</li> <li>- Mô tả: Lỗ hổng cho phép đối tượng tấn công truy cập và thực thi các hành vi trái phép.</li> <li>- Ảnh hưởng: OpenSSH.</li> <li>- Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.</li> </ul>	<a href="https://nvd.nist.gov/vuln/detail/CVE-2024-6387">https://nvd.nist.gov/vuln/detail/CVE-2024-6387</a>
2	CVE-2024-6327	<ul style="list-style-type: none"> <li>- Điểm CVSS: 9.8 (Nghiêm trọng)</li> <li>- Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã từ xa.</li> <li>- Ảnh hưởng: Progress Telerik Report Server</li> <li>- Lỗ hổng đang bị khai thác trong thực tế.</li> </ul>	<a href="https://nvd.nist.gov/vuln/detail/CVE-2024-6327">https://nvd.nist.gov/vuln/detail/CVE-2024-6327</a>
3	CVE-2023-45249	<ul style="list-style-type: none"> <li>- Điểm CVSS: 9.8 (Nghiêm trọng)</li> <li>- Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã từ xa.</li> </ul>	<a href="https://nvd.nist.gov/vuln/detail/CVE-2023-45249">https://nvd.nist.gov/vuln/detail/CVE-2023-45249</a>

		<ul style="list-style-type: none"> <li>- Ảnh hưởng: Acronis Cyber Infrastructure</li> <li>- Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.</li> </ul>	
4	CVE-2024-36401	<ul style="list-style-type: none"> <li>- Điểm CVSS: 9.8 (Nghiêm trọng)</li> <li>- Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã từ xa.</li> <li>- Ảnh hưởng: GeoServer</li> <li>- Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.</li> </ul>	<a href="https://nvd.nist.gov/vuln/detail/CVE-2024-36401">https://nvd.nist.gov/vuln/detail/CVE-2024-36401</a>
5	CVE-2024-23692	<ul style="list-style-type: none"> <li>- Điểm CVSS: 9.8 (Nghiêm trọng)</li> <li>- Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã từ xa.</li> <li>- Ảnh hưởng: Rejetto HTTP File Server</li> <li>- Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.</li> </ul>	<a href="https://nvd.nist.gov/vuln/detail/CVE-2024-23692">https://nvd.nist.gov/vuln/detail/CVE-2024-23692</a>
6	CVE-2024-38112	<ul style="list-style-type: none"> <li>- Điểm CVSS: 7.5 (Cao)</li> <li>- Mô tả: Lỗ hổng cho phép đối tượng tấn công truy cập và thực thi các hành vi trái phép.</li> <li>- Ảnh hưởng: Windows 10, Windows 11, Windows Server 2008, Windows Server 2012, Windows Server 2016, Windows Server 2019, Windows Server 2022.</li> <li>- Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.</li> </ul>	<a href="https://nvd.nist.gov/vuln/detail/CVE-2024-38112">https://nvd.nist.gov/vuln/detail/CVE-2024-38112</a>
7	CVE-2024-37085	<ul style="list-style-type: none"> <li>- Điểm CVSS: 6.8 (Cao)</li> <li>- Mô tả: Lỗ hổng cho phép đối tượng tấn công truy cập và thực thi các hành vi trái phép.</li> <li>- Ảnh hưởng: VMware ESXi</li> <li>- Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.</li> </ul>	<a href="https://nvd.nist.gov/vuln/detail/CVE-2024-37085">https://nvd.nist.gov/vuln/detail/CVE-2024-37085</a>
8	CVE-2024-36991	<ul style="list-style-type: none"> <li>- Điểm CVSS: 7.5 (Cao)</li> </ul>	<a href="https://nvd.nist.gov/vuln/detail/CVE-2024-36991">https://nvd.nist.gov/vuln/detail/CVE-2024-36991</a>

		<ul style="list-style-type: none"> <li>- Mô tả: Lỗ hổng cho phép đối tượng tấn công truy cập và thực thi các hành vi trái phép.</li> <li>- Ảnh hưởng: Splunk Enterprise trên Windows.</li> <li>- Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.</li> </ul>	
9	CVE-2006-5051	<ul style="list-style-type: none"> <li>- Điểm CVSS: 8.1 (Cao)</li> <li>- Mô tả: Lỗ hổng cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ, thực thi mã từ xa.</li> <li>- Ảnh hưởng: OpenSSH.</li> <li>- Lỗ hổng đang bị khai thác trong thực tế.</li> </ul>	<a href="https://nvd.nist.gov/vuln/detail/CVE-2006-5051">https://nvd.nist.gov/vuln/detail/CVE-2006-5051</a>
10	CVE-2024-20419	<ul style="list-style-type: none"> <li>- Điểm CVSS: 10.0 (Nghiêm trọng)</li> <li>- Mô tả: Lỗ hổng cho phép đối tượng tấn công truy cập và thực thi các hành vi trái phép.</li> <li>- Ảnh hưởng: Cisco Smart Software Manager On-Prem</li> <li>- Lỗ hổng đang bị khai thác trong thực tế.</li> </ul>	<a href="https://nvd.nist.gov/vuln/detail/CVE-2024-20419">https://nvd.nist.gov/vuln/detail/CVE-2024-20419</a>
11	CVE-2024-20401	<ul style="list-style-type: none"> <li>- Điểm CVSS: 9.8 (Nghiêm trọng)</li> <li>- Mô tả: Lỗ hổng cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ, thực thi mã từ xa, truy cập và thực thi các hành vi trái phép</li> <li>- Ảnh hưởng: Cisco Secure Email Gateway</li> <li>- Lỗ hổng đang bị khai thác trong thực tế.</li> </ul>	<a href="https://nvd.nist.gov/vuln/detail/CVE-2024-20401">https://nvd.nist.gov/vuln/detail/CVE-2024-20401</a>
12	CVE-2024-21412	<ul style="list-style-type: none"> <li>- Điểm CVSS: 8.1 (Cao)</li> <li>- Mô tả: Lỗ hổng cho phép đối tượng tấn công truy cập và thực thi các hành vi trái phép.</li> <li>- Ảnh hưởng: Windows 10, Windows 11, Windows 2019, Windows 2022.</li> <li>- Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.</li> </ul>	<a href="https://nvd.nist.gov/vuln/detail/CVE-2024-21412">https://nvd.nist.gov/vuln/detail/CVE-2024-21412</a>

## 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 1310/CATTT-NCSC ngày 12/7/2024 về việc lỗ hổng an toàn thông tin ảnh hưởng cao và nghiêm trọng trong các sản phẩm Microsoft công bố tháng 07/2024.

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.



IOC	NHÓM TẤN CÔNG APT
hxxp://sdfa.liveblog365[.]com/ares/babyhades.txt	Nhóm APT Kimsuky
hxxp://sdfa.liveblog365[.]com/ares/hades.txt	Nhóm APT Kimsuky
38e27983c757374d9bae36a2e2520e8e	Nhóm APT Kimsuky
bba3b15bad6b5a80ab9fa9a49b643658	Nhóm APT Kimsuky
193.239.86[.]168	Nhóm APT Ghost Emperor
imap.dateupdata[.]com	Nhóm APT Ghost Emperor
bab2ae2788dee2c41065850b2877202e57369f37	Nhóm APT Ghost Emperor

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 7/2024, Trung tâm NCSC phát hiện **19 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.



Phát hiện **100+** hệ thống bị lây nhiễm mã độc botnet trong tháng

TỔ CHỨC BỊ ẢNH HƯỞNG	ĐỊA CHỈ IP C&C	CỔNG KẾT NỐI C&C
...	216.218.185.162	80
...	216.218.185.162	80
...	216.218.185.162	80
...	216.218.185.162	80
Xem thêm		

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;
- PCT Trần Đăng Khoa;
- Các phòng: ATHTTT, TT&HTQT;
- Trung tâm VNCERT/CC;
- Lưu: VT, NCSC.LTQ.

**CỤC TRƯỞNG**

**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)*

<b>TT</b>	<b>Website giả mạo</b>	<b>Ghi chú</b>
1	<a href="https://shop[.]global-selling[.]top">https://shop[.]global-selling[.]top</a>	Website giả mạo sàn TMĐT Amazon
2	<a href="https://vn156475p[.]com">https://vn156475p[.]com</a>	Website giả mạo sàn TMĐT Amazon
3	<a href="https://vssid[.]govvn[.]com">https://vssid[.]govvn[.]com</a>	Website giả mạo Bảo hiểm Xã hội Việt Nam
4	<a href="https://vssidgov[.]com">https://vssidgov[.]com</a>	Website giả mạo Bảo hiểm Xã hội Việt Nam
5	<a href="https://baohiemxahoi[.]vnagov[.]com">https://baohiemxahoi[.]vnagov[.]com</a>	Website giả mạo Bảo hiểm Xã hội Việt Nam
6	<a href="https://vssid[.]govnn[.]cc/">https://vssid[.]govnn[.]cc/</a>	Website giả mạo Bảo hiểm Xã hội Việt Nam
7	<a href="https://mojgov[.]weebly[.]com">https://mojgov[.]weebly[.]com</a>	Website giả mạo Bộ Tư pháp
8	<a href="https://icchanoi[.]net/">https://icchanoi[.]net/</a>	Website giả mạo Công ty Cổ phần Đầu tư Quốc tế ICC Hà Nội
9	<a href="http://nappthe[.]vn">nappthe[.]vn</a>	Website giả mạo Công Ty Cổ phần Giải Trí Và Thể Thao Điện Tử Việt Nam
10	<a href="https://giiao[.]hangtietkiem[.]com">https://giiao[.]hangtietkiem[.]com</a>	Website giả mạo Công ty cổ phần giao hàng tiết kiệm
11	<a href="https://vgiao[.]hangtietkiem[.]com/">https://vgiao[.]hangtietkiem[.]com/</a>	Website giả mạo Công ty cổ phần giao hàng tiết kiệm
12	<a href="http://bachhoaxanh[.]com">bachhoaxanh[.]com</a>	Website giả mạo Công ty cổ phần Thương mại Bách Hóa Xanh

13	<a href="https://homecredit[.]hethongvaynhanh247[.]com/">https://homecredit[.]hethongvaynhanh247[.]com/</a>	Website giả mạo Công ty Tài chính TNHH MTV Home Credit Việt Nam
14	<a href="https://nqsncoau[.]buzz/">https://nqsncoau[.]buzz/</a>	Website giả mạo Cty tài chính TNHH ngân hàng Việt Nam Thịnh Vượng smbc
15	<a href="https://dienmayxanhctv24[.]com">https://dienmayxanhctv24[.]com</a>	Website giả mạo Điện máy xanh
16	<a href="https://thisinhthanhlich2024[.]com">https://thisinhthanhlich2024[.]com</a>	Website giả mạo Facebook
17	<a href="https://binhchoncuocthivetransinhvien2024[.]weebly[.]com">https://binhchoncuocthivetransinhvien2024[.]weebly[.]com</a>	Website giả mạo Facebook
18	<a href="https://mfacebook-com[.]vn/">https://mfacebook-com[.]vn/</a>	Website giả mạo Facebook
19	<a href="https://bethivetranh2024[.]weebly[.]com">https://bethivetranh2024[.]weebly[.]com</a>	Website giả mạo Facebook
20	<a href="https://events[.]pubg-vnggame[.]com">https://events[.]pubg-vnggame[.]com</a>	Website giả mạo Facebook
21	<a href="https://duyetdonlazada[.]com">https://duyetdonlazada[.]com</a>	Website giả mạo sàn TMĐT Lazada
22	<a href="https://da8975[.]com">https://da8975[.]com</a>	Website giả mạo sàn TMĐT Lazada
23	<a href="https://la5959[.]com">https://la5959[.]com</a>	Website giả mạo sàn TMĐT Lazada
24	<a href="https://www[.]lazada[.]com/">https://www[.]lazada[.]com/</a>	Website giả mạo sàn TMĐT Lazada
25	<a href="https://www[.]hethongnhanvien[.]com">https://www[.]hethongnhanvien[.]com</a>	Website giả mạo sàn TMĐT Lazada
26	<a href="https://da1215[.]com">https://da1215[.]com</a>	Website giả mạo sàn TMĐT Lazada
27	<a href="https://lazadaevent[.]com/">https://lazadaevent[.]com/</a>	Website giả mạo sàn TMĐT Lazada
28	<a href="https://lzdkiemdon24[.]com">https://lzdkiemdon24[.]com</a>	Website giả mạo sàn TMĐT Lazada

29	<a href="https://www[.]momoshopvip[.]com">https://www[.]momoshopvip[.]com</a>	Website giả mạo MoMo
30	<a href="https://www[.]baovietcom[.]vip/">https://www[.]baovietcom[.]vip/</a>	Website giả mạo Ngân hàng TMCP Bảo Việt
31	<a href="https://www[.]baovietn[.]vip">https://www[.]baovietn[.]vip</a>	Website giả mạo Ngân hàng TMCP Bảo Việt
32	<a href="http://moneytracking137[.]com">moneytracking137[.]com</a>	Website giả mạo Ngân Hàng TMCP Công Thương Việt Nam
33	<a href="https://vietinbankamc[.]vn">https://vietinbankamc[.]vn</a>	Website giả mạo Ngân Hàng TMCP Công Thương Việt Nam
34	<a href="https://tcbanhan[.]com">https://tcbanhan[.]com</a>	Website giả mạo Ngân hàng TMCP Kỹ Thương Việt Nam
35	<a href="https://khtechcanhan[.]com/">https://khtechcanhan[.]com/</a>	Website giả mạo Ngân hàng TMCP Kỹ Thương Việt Nam
36	<a href="https://vietcombank-career[.]com">https://vietcombank-career[.]com</a>	Website giả mạo Ngân Hàng TMCP Ngoại thương Việt Nam
37	<a href="http://cskhcanhanhd[.]com">cskhcanhanhd[.]com</a>	Website giả mạo Ngân hàng TMCP Phát triển Thành phố Hồ Chí Minh
38	<a href="http://hdbank[.]tructuyen-uudai-thekhachhang[.]com">hdbank[.]tructuyen-uudai-thekhachhang[.]com</a>	Website giả mạo Ngân hàng TMCP Phát triển Thành phố Hồ Chí Minh
39	<a href="https://vnmcrd2s[.]online">https://vnmcrd2s[.]online</a>	Website giả mạo Ngân hàng TMCP Quân đội
40	<a href="https://mbdk99[.]com">https://mbdk99[.]com</a>	Website giả mạo Ngân hàng TMCP Quân đội
41	<a href="https://www[.]dangnhaphoso[.]com">https://www[.]dangnhaphoso[.]com</a>	Website giả mạo Ngân hàng TMCP Quân đội
42	<a href="https://tcvnhomefic[.]com">https://tcvnhomefic[.]com</a>	Website giả mạo Ngân hàng TMCP Quân đội
43	<a href="https://mcqdv[.]com">https://mcqdv[.]com</a>	Website giả mạo Ngân hàng TMCP Quân đội
44	<a href="https://mmb-online[.]com">https://mmb-online[.]com</a>	Website giả mạo Ngân hàng TMCP Quân đội

45	vib-care[.]com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
46	http://dich-vu-the-sat-vib[.]com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
47	https://vib[.]chamsockhachhang-uudai-tructuyenthe[.]com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
48	http://dich-vu-the-elite-vib[.]com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
49	https://vib[.]chamsockhachhang-tructuyenuudai[.]online	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
50	dich-vu-the-vvip-vib[.]com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
51	visa-vibbank[.]com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
52	https://dich-vu-the-svip-vib[.]com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
53	https://nang-cap-ocare-vib[.]com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
54	vib-nangcap[.]com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
55	main-card-vib[.]com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
56	vib-up-the[.]shop	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
57	vib-cardnew[.]shop	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
58	vib-nang-the[.]com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
59	nang-cap-the-vcare-vib[.]com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
60	nang-cap-qcare-vib[.]com	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
61	vib-solution[.]shop	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam

62	<a href="http://vib[.]uudaikhachhang-tructuyen[.]com[.]vn">http://vib[.]uudaikhachhang-tructuyen[.]com[.]vn</a>	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
63	<a href="http://ib-miles-card[.]shop">http://ib-miles-card[.]shop</a>	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
64	<a href="http://vib-gold-card[.]shop">http://vib-gold-card[.]shop</a>	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
65	<a href="http://nang-hang-the-vip2-vib[.]com">http://nang-hang-the-vip2-vib[.]com</a>	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
66	<a href="http://nang-hang-the-vip3-vib[.]com">http://nang-hang-the-vip3-vib[.]com</a>	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
67	<a href="http://vib-khcn[.]shop/">http://vib-khcn[.]shop/</a>	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
68	<a href="http://vib-town[.]com">vib-town[.]com</a>	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
69	<a href="https://tpbank[.]chamsockhachhang-uudaithe-thang6[.]com">https://tpbank[.]chamsockhachhang-uudaithe-thang6[.]com</a>	Website giả mạo Ngân hàng TMCP Tiên Phong
70	<a href="http://www[.]vpbank[.]chamsockhachhang-uudaithecanhan-tructuyen[.]online">www[.]vpbank[.]chamsockhachhang-uudaithecanhan-tructuyen[.]online</a>	Website giả mạo Ngân hàng TMCP Việt Nam Thịnh Vượng
71	<a href="http://vpbank[.]uudai-tructuyen-chamsockhachhang-the[.]com[.]vn">vpbank[.]uudai-tructuyen-chamsockhachhang-the[.]com[.]vn</a>	Website giả mạo Ngân hàng TMCP Việt Nam Thịnh Vượng
72	<a href="https://www[.]vpbank[.]chamsockhachhang-uudai-the-truc-tuyen[.]online">https://www[.]vpbank[.]chamsockhachhang-uudai-the-truc-tuyen[.]online</a>	Website giả mạo Ngân hàng TMCP Việt Nam Thịnh Vượng
73	<a href="https://www[.]tinchapshinhan[.]online">https://www[.]tinchapshinhan[.]online</a>	Website giả mạo Ngân hàng TNHH MTV Shinhan Việt Nam
74	<a href="https://centralmarketing[.]online/">https://centralmarketing[.]online/</a>	Website giả mạo Ngân hàng Worldbank Việt Nam
75	<a href="https://lapdatinternet[.]net/">https://lapdatinternet[.]net/</a>	Website giả mạo SCTV
76	<a href="https://sendotv[.]com">https://sendotv[.]com</a>	Website giả mạo sàn TMĐT Sendo
77	<a href="https://sp75193p[.]com">https://sp75193p[.]com</a>	Website giả mạo sàn TMĐT Shopee
78	<a href="https://sp1663p[.]com">https://sp1663p[.]com</a>	Shopee

79	<a href="https://www[.]vn999mall[.]vip">https://www[.]vn999mall[.]vip</a>	Website giả mạo sàn TMĐT Shopee
80	<a href="https://sp1776p[.]com">https://sp1776p[.]com</a>	Website giả mạo sàn TMĐT Shopee
81	<a href="https://sp7335p[.]com">sp7335p[.]com</a>	Website giả mạo sàn TMĐT Shopee
82	<a href="https://vnc63661s[.]com">https://vnc63661s[.]com</a>	Website giả mạo sàn TMĐT Shopee
83	<a href="https://www[.]seleeshopee[.]com">https://www[.]seleeshopee[.]com</a>	Website giả mạo sàn TMĐT Shopee
84	<a href="https://vnc75635s[.]com">https://vnc75635s[.]com</a>	Website giả mạo sàn TMĐT Shopee
85	<a href="https://vnc69977s[.]com">https://vnc69977s[.]com</a>	Website giả mạo sàn TMĐT Shopee
86	<a href="https://www[.]shopeesop[.]com">https://www[.]shopeesop[.]com</a>	Website giả mạo sàn TMĐT Shopee
87	<a href="https://nze98582s[.]com/">https://nze98582s[.]com/</a>	Website giả mạo sàn TMĐT Shopee
88	<a href="https://odz68254s[.]com">https://odz68254s[.]com</a>	Website giả mạo sàn TMĐT Shopee
89	<a href="https://soppe86[.]life">https://soppe86[.]life</a>	Website giả mạo sàn TMĐT Shopee
90	<a href="https://www[.]sp5118p[.]com">https://www[.]sp5118p[.]com</a>	Website giả mạo sàn TMĐT Shopee
91	<a href="https://www[.]govgdt[.]top">https://www[.]govgdt[.]top</a>	Website giả mạo Tập đoàn Điện lực Việt Nam (EVN)
92	<a href="https://www[.]thanhtraptcrt[.]online">https://www[.]thanhtraptcrt[.]online</a>	Website giả mạo Thanh tra Chính phủ
93	<a href="https://fajiafu50[.]com">https://fajiafu50[.]com</a>	Website giả mạo sàn TMĐT Tiki
94	<a href="https://vntiki1[.]com">https://vntiki1[.]com</a>	Website giả mạo sàn TMĐT Tiki
95	<a href="https://tdkt00[.]com">https://tdkt00[.]com</a>	Website giả mạo sàn TMĐT Tiki

96	<a href="https://zla653[.]top">https://zla653[.]top</a>	Website giả mạo sản TMĐT Tiki
97	<a href="https://tdkt04[.]com">https://tdkt04[.]com</a>	Website giả mạo sản TMĐT Tiki
98	<a href="https://s2rjtiki[.]com">https://s2rjtiki[.]com</a>	Website giả mạo sản TMĐT Tiki
99	<a href="https://k2rjtiki[.]com">https://k2rjtiki[.]com</a>	Website giả mạo sản TMĐT Tiki
100	<a href="https://sh2tiki[.]com">https://sh2tiki[.]com</a>	Website giả mạo sản TMĐT Tiki
101	<a href="https://tdkt06[.]com">https://tdkt06[.]com</a>	Website giả mạo sản TMĐT Tiki
102	<a href="https://fajiafu30[.]com/">https://fajiafu30[.]com/</a>	Website giả mạo sản TMĐT Tiki
103	<a href="https://tdkt07[.]com">https://tdkt07[.]com</a>	Website giả mạo sản TMĐT Tiki
104	<a href="https://tikijaj2[.]com">https://tikijaj2[.]com</a>	Website giả mạo sản TMĐT Tiki
105	<a href="https://tikt88[.]com">https://tikt88[.]com</a>	Website giả mạo sản TMĐT Tiki
106	<a href="https://businesseventskp[.]top">https://businesseventskp[.]top</a>	Website giả mạo sản TMĐT Tiki
107	<a href="https://www[.]tikifreeship[.]vip/">https://www[.]tikifreeship[.]vip/</a>	Website giả mạo sản TMĐT Tiki
108	<a href="https://tdke00[.]com/">https://tdke00[.]com/</a>	Website giả mạo sản TMĐT Tiki
109	<a href="https://www[.]vntiki[.]vip">https://www[.]vntiki[.]vip</a>	Website giả mạo sản TMĐT Tiki
110	<a href="https://tdke02[.]com">https://tdke02[.]com</a>	Website giả mạo sản TMĐT Tiki
111	<a href="https://nhanvientiki[.]org">https://nhanvientiki[.]org</a>	Website giả mạo sản TMĐT Tiki
112	<a href="https://muasamtiki[.]com">https://muasamtiki[.]com</a>	Website giả mạo sản TMĐT Tiki



113	<a href="https://tracuutthvt[.]com">https://tracuutthvt[.]com</a>	Website giả mạo Tổng cục Thuế
114	<a href="http://chinhphu[.]cc">chinhphu[.]cc</a>	Website giả mạo Văn phòng Chính phủ
115	<a href="https://chinhphu[.]dancuquocgia[.]org">https://chinhphu[.]dancuquocgia[.]org</a>	Website giả mạo Văn phòng Chính phủ
116	<a href="https://viettlot135p[.]com">https://viettlot135p[.]com</a>	Website giả mạo Vietlott
117	<a href="http://quandoi-viettel[.]com">quandoi-viettel[.]com</a>	Website giả mạo Viettel
118	<a href="http://giaodichquoctes[.]com">Giaodichquoctes[.]com</a>	Website giả mạo Western Union
119	<a href="https://giaodichquoctes[.]vercel[.]app">https://giaodichquoctes[.]vercel[.]app</a>	Website giả mạo Western Union
120	<a href="https://giaodichquoctes[.]com">https://giaodichquoctes[.]com</a>	Website giả mạo Western Union
121	<a href="https://nhantienquoctev3[.]vercel[.]app/">https://nhantienquoctev3[.]vercel[.]app/</a>	Website giả mạo Western Union
122	<a href="https://chuyentienquoctenhanch[.]vercel[.]app/">https://chuyentienquoctenhanch[.]vercel[.]app/</a>	Website giả mạo Western Union
123	<a href="http://chuyentienquocte1313[.]vercel[.]app">chuyentienquocte1313[.]vercel[.]app</a>	Website giả mạo Western Union
124	<a href="http://giaodichdaquocgia[.]us">giaodichdaquocgia[.]us</a>	Website giả mạo Western Union
125	<a href="https://xacnhanthutuchoantra[.]us/">https://xacnhanthutuchoantra[.]us/</a>	Website giả mạo Western Union

**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	15834	<a href="https://nvd.nist.gov/vuln/detail/CVE-2022-26809">https://nvd.nist.gov/vuln/detail/ CVE-2022-26809</a>
2	CVE-2023-21716	6752	<a href="https://nvd.nist.gov/vuln/detail/CVE-2023-21716">https://nvd.nist.gov/vuln/detail/ CVE-2023-21716</a>
3	CVE-2023-29341	1408	<a href="https://nvd.nist.gov/vuln/detail/CVE-2023-29341">https://nvd.nist.gov/vuln/detail/ CVE-2023-29341</a>
4	CVE-2021-40444	995	<a href="https://nvd.nist.gov/vuln/detail/CVE-2021-40444">https://nvd.nist.gov/vuln/detail/ CVE-2021-40444</a>
5	CVE-2024-30093	958	<a href="https://nvd.nist.gov/vuln/detail/CVE-2024-30093">https://nvd.nist.gov/vuln/detail/ CVE-2024-30093</a>
6	CVE-2024-37985	807	<a href="https://nvd.nist.gov/vuln/detail/CVE-2024-37985">https://nvd.nist.gov/vuln/detail/ CVE-2024-37985</a>
7	CVE-2021-28310	786	<a href="https://nvd.nist.gov/vuln/detail/CVE-2021-28310">https://nvd.nist.gov/vuln/detail/ CVE-2021-28310</a>
8	CVE-2023-36732	725	<a href="https://nvd.nist.gov/vuln/detail/CVE-2023-36732">https://nvd.nist.gov/vuln/detail/ CVE-2023-36732</a>
9	CVE-2024-35265	579	<a href="https://nvd.nist.gov/vuln/detail/CVE-2024-35265">https://nvd.nist.gov/vuln/detail/ CVE-2024-35265</a>
10	CVE-2020-1097	565	<a href="https://nvd.nist.gov/vuln/detail/CVE-2020-1097">https://nvd.nist.gov/vuln/detail/ CVE-2020-1097</a>

**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	bba3b15bad6b5a80ab9fa9a49b643658	Nhóm APT Kimsuky
2	38e27983c757374d9bae36a2e2520e8e	
3	hxxp://sdfa.liveblog365[.]com/ares/hades.txt	
4	hxxp://sdfa.liveblog365[.]com/ares/abyhades.txt	
5	hxxp://ney.r-e[.]kr/mar/tys.txt	
6	hxxp://ney.r-e[.]kr/mar/tys.php	
7	hxxps://webman.w3school.cloudns[.]nz	
8	hxxps://onewithshare.blogspot[.]com/2023/04/10.html	
9	hxxps://raw.githubusercontent[.]com/HelperDav/Web/main/update.xml	
10	hxxps://github[.]com/cmastern	
11	0d068b6d0523f069d1ada59c12891c4a	Nhóm APT41
12	b3067f382d70705d4c8f6977a7d7bee4	
13	d72f202c1d684c9a19f075290a60920f	
14	294cc02db5a122e3a1bc4f07997956da	
15	393065ef9754e3f39b24b2d1051eab61	
16	bcac2cbda36019776d7861f12d9b59c4	

17	f062183da590aba5e911d2392bc29181	
18	4141c4b827ff67c180096ff5f2cc1474	
19	bc85062de0f70afd44bb072b0b71a8cc	
20	72070b165d1f11bd4d009a81bf28a3e5	
21	f0953ed4a679b987a2da95578873760 2	
22	hxxps[:]fullgasesspa[.]cl/tet/download[.] php	Nhóm APT VoidBanshee
23	hxxp[:]cbmelipilla[.]cl/te/test1[.]html	
24	hxxps[:]cbmelipilla[.]cl/te/hhhh2[.]php	
25	hxxps[:]hostalaskapatagonia[.]com/tt/te dfd[.]te	
26	hxxps[:]hostalaskapatagonia[.]com/tt/be come[.]txt	
27	hxxp[:]h[.]com:8000/test1[.]html	
28	185[.]172[.]128[.]95	
29	4bb191c6d3a234743ace703d7d518f8f	
30	43f1c44fa14f9ce2c0ba9451de2f7d3dd 1a208de	
31	95e3312de43c1da4cc3be8fa47ab9fa4	
32	a59cca28205eeb94c331010060f86ad2 f3d41882	
33	d8ebfd26bed0155e7c4ec2ca429c871d	
34	bab2ae2788dee2c41065850b2877202 e57369f37	
35	imap.dateupdata[.]com	
36	193.239.86[.]168	

37	45[.]66[.]217[.]106	Nhóm APT MirrorFace
38	45[.]77[.]12[.]212	
39	207[.]148[.]97[.]235	
40	64[.]176[.]214[.]51	
41	45[.]76[.]222[.]130	
42	207[.]148[.]90[.]45	
43	103[.]143[.]208[.]115	
44	103[.]143[.]209[.]36	
45	91[.]245[.]255[.]30	
46	89[.]233[.]109[.]69	
47	108[.]160[.]130[.]45	
48	95[.]85[.]91[.]15	
49	168[.]100[.]8[.]103	
50	45[.]77[.]183[.]161	
51	207[.]148[.]103[.]42	
52	103[.]143[.]208[.]29	
53	146[.]70[.]79[.]68	
54	91[.]245[.]255[.]79	
55	www[.]morrowadded[.]com	

56	www[.]lookpumrron[.]com	Nhóm APT MirrorFace
57	minggamevies[.]com	
58	2a12:a300:3600::31b5:2e02	
59	2400:8902::f03c:93ff:fe8a:5327	
60	93af6afb47f4c42bc0da3eedc6ecb9054 134f4a47ef0add0d285404984011072	
61	43349c97b59d8ba8e1147f911797220 b1b7b87609fe4aaa7f1dbacc2c27b361 d	
62	0d59734bdb0e6f4fe6a44312a2d55145 e98b00f75a148394b2e4b86436c32f4c	
63	572f6b98cc133b2d0c8a4fd8ff9d14ae3 6cdaa119086a5d56079354e49d2a7ce	
64	5e7cd0461817b390cf05a7c874e017e9 f44eef41e053da99b479a4dfa3a04512	
65	2001:19f0:7001:2ae2:5400:4ff:fe0a:55 66	
66	2a12:a300:3700::5d9f:b451	
67	bcd34d436cbac235b56ee5b7273baed6 2bf385ee13721c7fdcf00af9ed63997	
68	4f932d6e21fdd0072aba61203c731969 3e490adbd9e93a49b0fe870d4d0aed71	
69	9590646b32fec3aafd6c648f69ca9857f b4be2adf3bc321c8cd25ba7b83	
70	7a7e7e0d817042e54129697947dfb42 3b607692f4457163b5c62ffea69a8108 d	
71	b07c7dfb3617cd40edc1ab309a68489a 3aa4aa1e8fd486d047c155c952dc509e	

**Phụ lục IV**  
**DANH SÁCH CÁC ĐƠN VỊ CÓ ĐỊA CHỈ IP NẴM 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 06/2024	Số lượng IP botnet tháng 07/2024	Loại mã độc/botnet
1	Bảo hiểm Xã hội Việt Nam	1	1	Andromeda
2	Đài Tiếng nói Việt Nam	0	1	Andromeda

**2. Danh sách Tỉnh/thành**

STT	Tên đơn vị	Số lượng IP botnet tháng 06/2024	Số lượng IP botnet tháng 07/2024	Ghi chú
1	Hà Nam	3	5	Andromeda
2	Lâm Đồng	0	3	Andromeda
3	Lai Châu	6	2	Andromeda
4	Nam Định	2	2	Andromeda
5	Thanh Hóa	2	2	Andromeda
6	Thái Bình	1	2	Andromeda
7	Lạng Sơn	1	2	Andromeda
8	Ninh Bình	1	2	UrlZone, Andromeda
9	Điện Biên	0	2	Andromeda
10	Gia Lai	1	1	Andromeda

11	Hà Nội	1	1	Andromeda
12	Kon Tum	1	1	Andromeda
13	An Giang	0	1	Andromeda
14	Bà Rịa Vũng Tàu	0	1	Andromeda
15	Quảng Ninh	0	1	Andromeda
16	Đắk Nông	0	1	Andromeda
17	Cao Bằng	0	1	Andromeda



**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**

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

<b>18</b>	<b>Thanh tra Chính phủ</b>	<b>10/11/2020</b>	<b>Không nhận được dữ liệu chia sẻ</b>
19	Ủy ban Dân tộc	08/10/2020	31/07/2024
<b>20</b>	<b>Văn phòng Chính phủ</b>	<b>22/09/2020</b>	<b>Không nhận được dữ liệu chia sẻ</b>
21	Bảo Hiểm Xã Hội	08/11/2020	31/07/2024
22	Đài Truyền hình Việt Nam	14/09/2020	31/07/2024
23	Viện Hàn Lâm KHCN	22/09/2020	31/07/2024
<b>24</b>	<b>Kiểm toán Nhà nước Việt Nam</b>	<b>09/03/2021</b>	<b>22/07/2024</b>

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

27	Hà Tĩnh	06/10/2020	31/07/2024
28	Hòa Bình	13/05/2020	31/07/2024
29	Hồ Chí Minh	26/06/2020	31/07/2024
30	Hậu Giang	02/10/2020	31/07/2024
31	Hưng Yên	22/05/2020	31/07/2024
32	Khánh Hòa	21/09/2020	31/07/2024
33	Kiên Giang	24/09/2020	31/07/2024
34	Kon Tum	28/09/2020	31/07/2024
35	Lai Châu	26/09/2020	31/07/2024
36	Lâm Đồng	22/10/2020	31/07/2024
37	Lạng Sơn	08/10/2020	31/07/2024
38	Lào Cai	09/07/2020	31/07/2024
39	Long An	22/07/2020	31/07/2024
40	Nam Định	21/09/2020	31/07/2024
41	Nghệ An	09/09/2020	31/07/2024
42	Ninh Bình	28/07/2020	31/07/2024
43	Ninh Thuận	01/09/2020	31/07/2024
<b>44</b>	<b>Phú Thọ</b>	<b>01/10/2020</b>	<b>Không nhận được dữ liệu chia sẻ</b>
45	Phú Yên	30/11/2020	31/07/2024
46	Quảng Bình	01/07/2020	31/07/2024
<b>47</b>	<b>Quảng Nam</b>	<b>14/09/2020</b>	<b>Không nhận được dữ liệu chia sẻ</b>
48	Quảng Ngãi	12/08/2020	31/07/2024
<b>49</b>	<b>Quảng Ninh</b>	<b>12/09/2020</b>	<b>Không nhận được dữ liệu chia sẻ</b>
50	Quảng Trị	24/12/2020	31/07/2024
51	Sóc Trăng	12/08/2020	31/07/2024
52	Sơn La	13/07/2020	31/07/2024
53	Tây Ninh	08/07/2020	31/07/2024
54	Thái Bình	25/06/2020	31/07/2024
55	Thái Nguyên	19/11/2020	31/07/2024
56	Thanh Hóa	29/09/2020	31/07/2024

57	Thừa Thiên Huế	29/07/2020	31/07/2024
58	Tiền Giang	24/09/2020	31/07/2024
59	Trà Vinh	29/07/2020	31/07/2024
60	Tuyên Quang	19/11/2020	16/07/2024
61	Vĩnh Long	25/06/2020	31/07/2024
62	<b>Vĩnh Phúc</b>	<b>30/06/2020</b>	<b>Không nhận được dữ liệu chia sẻ</b>
63	Yên Bái	26/08/2020	31/07/2024

**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 07/2024	Ghi chú
1	Bộ Công Thương	196	
2	<b>Bộ Giáo dục và Đào tạo</b>	<b>0</b>	<b>Chưa chia sẻ</b>
3	Bộ Giao thông vận tải	85	
4	Bộ Kế hoạch và Đầu tư	1006	
5	Bộ Khoa học và Công nghệ	383	
6	<b>Bộ Lao động - Thương Binh và Xã hội</b>	<b>0</b>	<b>Mất kết nối 01 tháng trở lên</b>
7	Bộ Ngoại giao	10	
8	Bộ Nội vụ	447	
9	<b>Bộ Nông nghiệp và Phát triển nông thôn</b>	<b>0</b>	<b>Chưa chia sẻ</b>
10	Bộ Tài chính	278	
11	Bộ Tài nguyên và Môi trường	56	
12	Bộ Thông tin và Truyền thông	243	
13	Bộ Tư pháp	8388	
14	Bộ Văn hóa, Thể thao và Du lịch	25	
15	Bộ Xây Dựng	31	
16	Bộ Y tế	54	

17	Ngân hàng Nhà nước Việt Nam	3533	
<b>18</b>	<b>Thanh tra Chính phủ</b>	<b>0</b>	<b>Mất kết nối 01 tháng trở lên</b>
<b>19</b>	<b>Ủy ban Dân tộc</b>	<b>0</b>	<b>Chưa chia sẻ</b>
<b>20</b>	<b>Văn phòng Chính phủ</b>	<b>0</b>	<b>Mất kết nối 01 tháng trở lên</b>
21	Ban Quản lý Lăng Chủ tịch Hồ Chí Minh	3	
22	Bảo Hiểm Xã Hội	14600	
23	Đài tiếng nói Việt Nam	16	
24	Đài Truyền hình Việt Nam	177	
25	Thông tấn xã Việt Nam	1699	
26	Viện Hàn Lâm KHCN	114	
27	Viện Hàn Lâm KHXH	156	
<b>28</b>	<b>Kiểm toán Nhà nước Việt Nam</b>	<b>0</b>	<b>Mất kết nối 01 tháng trở lên</b>

**2. Danh sách Tỉnh/Thành**

<b>TT</b>	<b>Tỉnh/Thành</b>	<b>Số lượng máy chia sẻ dữ liệu trong tháng 07/2024</b>	<b>Ghi chú</b>
1	An Giang	460	
2	Bắc Giang	1180	
3	Bắc Kạn	3067	
4	Bạc Liêu	1914	
5	Bắc Ninh	1593	
6	Bà Rịa - Vũng Tàu	22877	
7	Bến Tre	37	
8	Bình Định	164	
9	Bình Dương	8966	
10	Bình Phước	4035	
11	Bình Thuận	3360	
12	Cà Mau	1847	
13	Cần Thơ	1499	
14	Cao Bằng	1291	
15	Đắk Lắk	5202	
16	Đắk Nông	1243	



17	Đà Nẵng	54083	
18	Điện Biên	4025	
<b>19</b>	<b>Đồng Nai</b>	<b>0</b>	<b>Mất kết nối 01 tháng trở lên</b>
20	Đồng Tháp	8859	
21	Gia Lai	20	
22	Hà Giang	13	
23	Hải Dương	2096	
24	Hải Phòng	2723	
25	Hà Nam	920	
26	Hà Nội	6239	
27	Hà Tĩnh	2027	
28	Hòa Bình	862	
29	Hồ Chí Minh	1	
30	Hậu Giang	974	
31	Hưng Yên	552	
32	Khánh Hòa	2881	
33	Kiên Giang	3457	
34	Kon Tum	4778	

35	Lai Châu	34	
36	Lâm Đồng	2496	
37	Lạng Sơn	325	
38	Lào Cai	3	
39	Long An	2690	
40	Nam Định	42	
41	Nghệ An	5093	
42	Ninh Bình	150	
43	Ninh Thuận	909	
44	Phú Thọ	1	
45	Phú Yên	136	
46	Quảng Bình	2491	
47	Quảng Nam	242	
48	Quảng Ngãi	3671	
<b>49</b>	<b>Quảng Ninh</b>	<b>0</b>	<b>Mất kết nối 01 tháng trở lên</b>
50	Quảng Trị	318	
51	Sóc Trăng	34	
52	Sơn La	4204	

53	Tây Ninh	1371	
54	Thái Bình	3554	
55	Thái Nguyên	2067	
56	Thanh Hóa	1739	
57	Thừa Thiên Huế	5970	
58	Tiền Giang	31461	
59	Trà Vinh	1273	
60	Tuyên Quang	3347	
61	Vĩnh Long	3276	
62	Vĩnh Phúc	11891	
63	Yên Bái	1024	

**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).