

Số: /BC-CATTT

Hà Nội, ngày tháng năm 2024

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

Thực hiện chức năng quản lý nhà nước và tổ chức thực thi pháp luật về an toàn thông tin mạng, Cục An toàn thông tin phát hành Báo cáo An toàn thông tin định kỳ hàng tháng.

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

Trong tháng 4/2024, Cục An toàn thông tin (Bộ Thông tin và Truyền thông) phát hiện xu hướng tấn công mạng mã hóa tống tiền (ransomware) tăng cao. Đã có một số hệ thống thông tin của cơ quan, tổ chức, doanh nghiệp tại Việt Nam bị sự cố tấn công, gây gián đoạn hoạt động và thiệt hại về vật chất, hình ảnh của các cơ quan, tổ chức, doanh nghiệp, cũng như hoạt động bảo đảm an toàn không gian mạng quốc gia.

Trong tháng 4/2024, hệ thống giám sát, cảnh báo sớm rủi ro của Trung tâm NCSC đã ghi nhận hàng trăm tên miền giả mạo các cơ quan, tổ chức tài chính, các ngân hàng nhằm mục tiêu lừa đảo người dân trên không gian mạng. Về nguy cơ, rủi ro mới, NCSC ghi nhận **12 lỗ hổng mới** có thể gây ra các nguy cơ **Nghiêm Trọng** đến hệ thống thông tin. Trung tâm NCSC cũng đã phân tích và công bố danh sách các chỉ báo tấn công mạng (IoC) liên quan đến các chiến dịch tấn công có thể ảnh hưởng đến Việt Nam đến các đơn vị.

Đề nghị các đơn vị, tổ chức, doanh nghiệp nghiên cứu các thông tin về các nguy cơ rủi ro trong báo cáo, thực hiện rà soát hệ thống, xử lý các vấn đề về an toàn thông tin mạng trong hệ thống và gửi kết quả báo cáo rà soát về địa chỉ thư điện tử **[ncsc@ais.gov.vn](mailto:ncsc@ais.gov.vn)** **chậm nhất trước ngày 15 hàng tháng.**

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



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

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



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

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

Thực hiện công tác kiểm tra, rà soát an toàn thông tin trên không gian mạng, Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC) đã ghi nhận **124.624 địa chỉ website** giả mạo cơ quan, tổ chức. Các đối tượng sử dụng website giả mạo này để lừa đảo, gây thiệt hại cho người dân trên không gian mạng, đồng thời gây thiệt hại nghiêm trọng đến uy tín, thương hiệu của chính cơ quan, tổ chức bị giả mạo.

Mục tiêu hướng đến của các đối tượng lừa đảo là lừa đảo người dân thông qua giả mạo các website của cơ quan chức năng, các tổ chức tài chính – ngân hàng, các sàn thương mại điện tử, các công ty lớn...

Trong tháng 4/2024, hệ thống của NCSC đã phát hiện 42 website giả mạo thương hiệu với mục đích lừa đảo được phát tán trên không gian mạng. Đề nghị các đơn vị, tổ chức, doanh nghiệp cần chủ động rà quét, phát hiện sớm các website lừa đảo giả mạo tổ chức của mình, cảnh báo sớm đến người dùng của mình nhằm ngăn chặn các hoạt động lừa đảo đến người dùng, đảm bảo an toàn thông tin cho người dùng, bảo vệ chính thương hiệu của tổ chức.



WEBSITE	ĐỊA CHỈ IP	GIẢ MẠO TỔ CHỨC
https://tdkd08[.]com/ <small>sản TMDT Tiki</small>		Website giả mạo sản TMDT Tiki
https://canhanshinhan[.]com <small>Ngân hàng TMĐT MTV Shinhan Việt Nam</small>		Website giả mạo Ngân hàng TNHH MTV Shinhan Việt Nam
https://vnsendo[.]shop/ <small>sản TMDT Sendo</small>		Website giả mạo sản TMDT Sendo
https://www[.]dailysshopee[.]com <small>sản TMDT Shopee</small>		Website giả mạo sản TMDT Shopee
https://vn63251s[.]com <small>sản TMDT Shopee</small>		Website giả mạo sản TMDT Shopee

*Danh sách các website lừa đảo được cập nhật tại  
<https://alert.khonggianmang.vn/>*

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

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

Thực hiện nhiệm vụ thu thập thông tin, tổng hợp, phân tích, theo dõi và dự báo, cảnh báo sớm xu hướng về các hoạt động, diễn biến trên không gian mạng Việt Nam. Trong tháng, Hệ thống giám sát kỹ thuật của NCSC đã ghi nhận có 89.351 điểm yếu, lỗ hổng an toàn thông tin tại các máy chủ, máy trạm, hệ thống thông tin của các cơ quan tổ chức nhà nước.

**Ghi chú:** Danh sách TOP 10 điểm yếu, lỗ hổng tồn tại phổ biến trên các máy của cơ quan, tổ chức tại Phụ lục II kèm theo.

Trong tháng 4/2024, hệ thống giám sát, rà quét từ xa của Trung tâm NCSC đã phát hiện hơn 1600 lỗ hổng trên 5000 hệ thống đang mở công khai trên Internet. Trung tâm NCSC cũng đã ghi nhận 12 lỗ hổng mới được công bố, có mức độ ảnh hưởng **Nghiêm trọng/Cao** có thể bị lợi dụng để tấn công, khai thác vào các hệ thống của các cơ quan, tổ chức. Các lỗ hổng này là các lỗ hổng tồn tại trên các sản phẩm phổ biến của nhiều cơ quan, tổ chức, doanh nghiệp. Đề nghị các đơn vị cần thực hiện kiểm tra toàn diện và rà soát hệ thống của mình giúp xác định hệ thống của mình có sử dụng các sản phẩm bị ảnh hưởng bởi các lỗ hổng không, nhanh chóng đưa ra biện pháp khắc phục kịp thời để bảo vệ an toàn thông tin.

Đồng thời, liên tục cập nhật thông tin về các lỗ hổng mới, các xu hướng tấn công trên không gian mạng.



Danh sách các lỗ hổng mới được cập nhật tại <https://alert.khonggianmang.vn/>

**Thông kê các lỗ hổng đáng chú ý được ghi nhận trong tháng 4/2024:**

TT	Mã điểm yếu/lỗ hổng	Mô tả	Ghi chú
1	CVE-2024-3094	<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 hiện các hành vi trái phép.</li> <li>- Ảnh hưởng: Tukaani XZ</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-2024-3094">https://nvd.nist.gov/vuln/detail/CVE-2024-3094</a>
2	CVE-2024-21894	<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 tùy ý.</li> <li>- Ảnh hưởng: Ivanti Connect Secure, Ivanti Policy Secure</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-2024-21894">https://nvd.nist.gov/vuln/detail/CVE-2024-21894</a>
3	CVE-2024-3400	<ul style="list-style-type: none"> <li>- Điểm CVSS: 10 (Nghiêm trọng)</li> <li>- Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã tùy ý.</li> <li>- Ảnh hưởng: Palo Alto Networks PAN-OS</li> </ul>	<a href="https://nvd.nist.gov/vuln/detail/CVE-2024-3400">https://nvd.nist.gov/vuln/detail/CVE-2024-3400</a>

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

9	CVE-2024-22023	<ul style="list-style-type: none"> <li>- Điểm CVSS: 5.3 (Trung bình)</li> <li>- Mô tả: Lỗi hỏng cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ.</li> <li>- Ảnh hưởng: Ivanti Connect Secure, Ivanti Policy Secure</li> <li>- Lỗi hỏng hiện đang bị khai thác trong thực tế.</li> </ul>	<a href="https://nvd.nist.gov/vuln/detail/CVE-2024-22023">https://nvd.nist.gov/vuln/detail/CVE-2024-22023</a>
10	CVE-2024-22053	<ul style="list-style-type: none"> <li>- Điểm CVSS: 8.2 (Cao)</li> <li>- Mô tả: Lỗi hỏng cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ.</li> <li>- Ảnh hưởng: Ivanti Connect Secure, Ivanti Policy Secure</li> <li>- Lỗi hỏng hiện đang bị khai thác trong thực tế.</li> </ul>	<a href="https://nvd.nist.gov/vuln/detail/CVE-2024-22053">https://nvd.nist.gov/vuln/detail/CVE-2024-22053</a>
11	CVE-2024-22052	<ul style="list-style-type: none"> <li>- Điểm CVSS: 7.5 (Cao)</li> <li>- Mô tả: Lỗi hỏng cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ.</li> <li>- Ảnh hưởng: Ivanti Connect Secure, Ivanti Policy Secure</li> <li>- Lỗi hỏng hiện đang bị khai thác trong thực tế.</li> </ul>	<a href="https://nvd.nist.gov/vuln/detail/CVE-2024-22052">https://nvd.nist.gov/vuln/detail/CVE-2024-22052</a>
12	CVE-2024-21893	<ul style="list-style-type: none"> <li>- Điểm CVSS: 8.2 (Cao)</li> <li>- Mô tả: Lỗi hỏng cho phép đối tượng tấn công khai thác lỗi SSRF.</li> <li>- Ảnh hưởng: Ivanti Connect Secure, Ivanti Policy Secure.</li> <li>- Lỗi hỏng hiện đang bị khai thác trong thực tế.</li> </ul>	<a href="https://nvd.nist.gov/vuln/detail/CVE-2024-21893">https://nvd.nist.gov/vuln/detail/CVE-2024-21893</a>

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

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

mạng quốc gia. Cục An toàn thông tin đã phát hành Công văn số 607/CATTT-NCSC ngày 17/04/2024 về việc lỗ hổng bảo mật ảnh hưởng nghiêm trọng trong phần mềm PAN-OS; công văn số 722/CATTT-NCSC ngày 24/04/2024 về việc cảnh báo phát hiện mã độc trojan Redline Stealer gây ảnh hưởng trên các hệ thống thông tin.

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



IOC	NHÓM TẤN CÔNG APT
advanced-ipsccanner[.]com	FIN7
109[.]107.171[.]162	FIN7
185[.]39.204[.]179	FIN7
166[.]1.160[.]118	FIN7
181[.]215.69[.]124	FIN7
myscannappo[.]online	FIN7
myscannappo[.]info	FIN7

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

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

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

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

Trong tháng 4/2024, Trung tâm NCSC phát hiện **05 hệ thống** của các đơn vị có kết nối đến hạ tầng botnet. Trung tâm NCSC đã thực hiện chia sẻ các thông tin botnet này đến các đơn vị thông qua hệ thống phát hiện cảnh báo sớm botnet.



Phát hiện 5 hệ thống bị lấy nhiễm mã độc botnet trong tháng

TỔ CHỨC BỊ ẢNH HƯỞNG	ĐỊA CHỈ IP C&C	CÔNG KẾT NỐI C&C
	216.218.185.162	80
	216.218.185.162	80
	216.218.185.162	80
	216.218.185.162	80
	216.218.185.162	80
<a href="#">Xem thêm</a>		

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

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

Trong quá trình thực hiện, nếu có thông tin cần hỗ trợ đề nghị liên hệ với Trung tâm giám sát an toàn không gian mạng quốc gia, Cục An toàn thông tin, Bộ Thông tin và Truyền thông: điện thoại: 024.32091.616 hoặc số điện thoại trực đường dây nóng hỗ trợ giám sát, cảnh báo sớm 0961.405.333, thư điện tử: [ncsc@ais.gov.vn](mailto:ncsc@ais.gov.vn).

**Nơi nhận:**

- Như trên;
- Thứ trưởng Phạm Đức Long (đề b/c);
- Đơn vị chuyên trách về ATTT/CNTT của Văn phòng Trung ương Đảng, Văn phòng Quốc hội, Văn phòng Chủ tịch nước, Tòa án Nhân dân tối cao, Viện Kiểm sát nhân dân tối cao, Kiểm toán Nhà nước;
- Đơn vị chuyên trách về ATTT/CNTT của các bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ;
- Sở TT&TT các tỉnh, thành phố trực thuộc TW;
- Các Tập đoàn kinh tế và Tổng công ty nhà nước;
- Các Tổ chức tài chính, Ngân hàng thương mại nhà nước;
- Ngân hàng Thương mại cổ phần;
- Ngân hàng Chính sách xã hội;
- Ngân hàng Phát triển Việt Nam;
- Ngân hàng Hợp tác xã Việt Nam;
- Các công ty Cổ phần Chứng khoán;
- Các Tổ chức, doanh nghiệp hoạt động trong lĩnh vực thương mại điện tử;
- Các tổ chức, doanh nghiệp cung cấp dịch vụ trung gian thanh toán, ví điện tử;
- Các Cục: Viễn thông, Bưu điện Trung ương;
- Các Trung tâm: TTTT, VNNIC;
- Cục trưởng (đề b/c);
- Các Phó Cục trưởng;
- Các phòng: ATHTTT, TT&HTQT;
- Trung tâm VNCERT/CC;
- Lưu: VT, NCSC.LTQ.

**KT. CỤC TRƯỞNG  
PHÓ CỤC TRƯỞNG**

**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	<a href="https://www[.]vnambzuon36sc[.]vip/">https://www[.]vnambzuon36sc[.]vip/</a>	Website giả mạo sàn TMĐT Amazon
2	<a href="https://vn147258p[.]com">https://vn147258p[.]com</a>	Website giả mạo sàn TMĐT Amazon
3	<a href="https://quaysomedialmart2024[.]vip">https://quaysomedialmart2024[.]vip</a>	Website giả mạo Công ty Cổ phần MediaMart Việt Nam
4	<a href="https://quaysomedialmart2024[.]vip/">https://quaysomedialmart2024[.]vip/</a>	Website giả mạo Công ty Cổ phần MediaMart Việt Nam
5	<a href="https://hdtinchap[.]com">https://hdtinchap[.]com</a>	Website giả mạo Công ty Tài chính TNHH HD SAISON
6	<a href="https://mayxanhsupport[.]com/">https://mayxanhsupport[.]com/</a>	Website giả mạo Điện máy xanh
7	<a href="https://lotttemart[.]store">https://lotttemart[.]store</a>	Website giả mạo LOTTE
8	<a href="https://clzl[.]pro">https://clzl[.]pro</a>	Website giả mạo MoMo
9	<a href="https://vdbank[.]com[.]vn">https://vdbank[.]com[.]vn</a>	Website giả mạo Ngân hàng Phát triển Việt Nam
10	<a href="https://sotuyenvcb[.]vietcombank[.]com">https://sotuyenvcb[.]vietcombank[.]com</a>	Website giả mạo Ngân Hàng TMCP Ngoại thương Việt Nam
11	<a href="https://mbfic-plus[.]com">https://mbfic-plus[.]com</a>	Website giả mạo Ngân hàng TMCP Quân đội
12	<a href="https://khach-hang-ca-nhan-vip5[.]com">https://khach-hang-ca-nhan-vip5[.]com</a>	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam
13	<a href="https://dich-vu-khcn-vvip-vib[.]com">https://dich-vu-khcn-vvip-vib[.]com</a>	Website giả mạo Ngân hàng TMCP Quốc tế Việt Nam

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

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

**Phụ lục II**  
**MỘT SỐ LỖ HỔNG VẤN CÒN TỒN TẠI PHỔ BIẾN TRÊN CÁC MÁY**  
**CỦA CƠ QUAN TỔ CHỨC**

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

TT	Mã điểm yếu/ lỗ hổng	SL máy bị ảnh hưởng	Ghi chú
1	CVE-2022-26809	15934	<a href="https://nvd.nist.gov/vuln/detail/CVE-2022-26809">https://nvd.nist.gov/vuln/detail/ CVE-2022-26809</a>
2	CVE-2024-3516	11294	<a href="https://nvd.nist.gov/vuln/detail/CVE-2024-3516">https://nvd.nist.gov/vuln/detail/ CVE-2024-3516</a>
3	CVE-2024-3914	10154	<a href="https://nvd.nist.gov/vuln/detail/CVE-2024-3914">https://nvd.nist.gov/vuln/detail/ CVE-2024-3914</a>
4	CVE-2024-2887	8555	<a href="https://nvd.nist.gov/vuln/detail/CVE-2023-2887">https://nvd.nist.gov/vuln/detail/ CVE-2023-2887</a>
5	CVE-2023-21716	6598	<a href="https://nvd.nist.gov/vuln/detail/CVE-2024-21716">https://nvd.nist.gov/vuln/detail/ CVE-2024-21716</a>
6	CVE-2024-4060	5045	<a href="https://nvd.nist.gov/vuln/detail/CVE-2024-4060">https://nvd.nist.gov/vuln/detail/ CVE-2024-4060</a>
7	CVE-2024-3865	3406	<a href="https://nvd.nist.gov/vuln/detail/CVE-2024-3965">https://nvd.nist.gov/vuln/detail/ CVE-2024-3965</a>
8	CVE-2024-3846	3346	<a href="https://nvd.nist.gov/vuln/detail/CVE-2024-3846">https://nvd.nist.gov/vuln/detail/ CVE-2024-3846</a>
9	CVE-2024-3159	2871	<a href="https://nvd.nist.gov/vuln/detail/CVE-2024-2871">https://nvd.nist.gov/vuln/detail/ CVE-2024-2871</a>
10	CVE-2022-0001	2771	<a href="https://nvd.nist.gov/vuln/detail/CVE-2024-2771">https://nvd.nist.gov/vuln/detail/ CVE-2024-2771</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	Update.py	CVE-2024-3400
2	3de2a4392b8715bad070b2a e12243f166ead37830f7c6d24e7 78985927f9caac	
3	5460b51da26c060727d128f3b3 d6415d1a4c25af6a29fef4cc6b8 67ad3659078	
4	172.233.228[.]93	
5	hxxp://172.233.228[.]93/policy	
6	hxxp://172.233.228[.]93/patch	
7	66.235.168[.]222	
8	5e37b3289054d5e774c02a6ec4 915a60156d715f3a02aaceb725 6cc3ebdc6610	Redline Stealer
9	https[:]//github[.]com/microsoft /vcpkg/files/14125503/Cheat.La b.2.7.2.zip	
10	873aa2e88dbc2efa089e6efd1c8 a5370e04c9f5749d7631f2912b cb640439997	
11	751f97824cd211ae710655e60a 26885cd79974f0f0a5e4e582e3b 635492b4cad	
12	dfbf23697cfd9d35f263af7a455 351480920a95bfc642f3254ee8 452ce20655a	
13	213[.]248[.]43[.]58	
14	hxxps://github.com/microsoft/S TL/files/14432565/Cheater.Pro. 1.6.0.zip	

15	51[.]79[.]208[.]192	CoralRaider
16	199[.]34[.]27[.]196	
17	139[.]99[.]23[.]9	
18	14[.]225[.]210[.]98	
19	14[.]225[.]210[.]97	
20	14[.]225[.]210[.]209	
21	14[.]225[.]210[.]222	
22	doc-0s-44- docstext[.]googleusercontent[.] com	
23	doc-10-44- docstext[.]googleusercontent[.] com	
24	kzeight8ht.top/upload.php	
25	kbeight8sb.top/upload.php	
26	kbeight8vs.top/upload.php	
27	kbeight8ht.top/upload.php	
28	kbeight8pn.top/upload.php	
29	dbeight8pt.top/zip.php	
30	kveight8sb.top/zip.php	
31	peasanthovecapsll.shop/api	
32	claimconcessionrebe.shop/api	
33	culturesketchfinanciall.shop/api	
34	gemcreedarticulateod.shop/api	
35	liabilityarrangemenyit.shop/api	
36	modestessayevenmilwek.shop/a pi	
37	secretionsuitcasenioise.shop/api	
38	sofahuntingslidedine.shop/api	
39	triangleseasonbenchwj.shop/api	
40	185.23.108.220 6339	
41	techsheck.b-cdn.net/Zen90	
42	zexodown-2.b-cdn.net/Peta12	
43	denv-2.b-cdn.net/Febl5	
44	metrodown-2.b-cdn.net/MebL1	
45	metrodown-2.b-cdn.net/SAq2	
46	denv-2.b-cdn.net/Febl4	

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



**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 03/2024	Số lượng IP botnet tháng 04/2024	Loại mã độc/botnet
1	Viện Hàn lâm Khoa học và Công nghệ Việt Nam	0	1	StealRat

**2. Danh sách Tỉnh/thành**

STT	Tên đơn vị	Số lượng IP botnet tháng 03/2024	Số lượng IP botnet tháng 04/2024	Ghi chú
1	Bà Rịa Vũng Tàu	1	1	Andromeda
2	Đắk Nông	0	1	Gamut
3	Lai Châu	2	1	Andromeda
4	Thái Bình	1	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 30/04/2024)</b>	<b>Số lượng cảnh báo trong tháng 04/2024</b>
<b>1</b>	<b>Bộ Công Thương</b>	<b>09/08/2020</b>	<b>29/04/2023</b>	<b>0</b>
<b>2</b>	<b>Bộ Giáo dục và Đào tạo</b>	<b>31/08/2020</b>	<b>09/01/2024</b>	<b>0</b>
<b>3</b>	<b>Bộ Giao thông vận tải</b>	<b>15/05/2020</b>	<b>26/07/2023</b>	<b>0</b>
4	Bộ Kế hoạch và Đầu tư	20/11/2020	23/04/2024	33289
5	Bộ Khoa học và Công nghệ	19/11/2020	15/04/2024	14717
<b>6</b>	<b>Bộ Lao động - Thương Binh và Xã hội</b>	<b>11/12/2020</b>	<b>03/10/2023</b>	<b>0</b>
7	Bộ Ngoại giao	24/07/2020	<b>22/01/2024</b>	<b>0</b>
<b>8</b>	<b>Bộ Nội vụ</b>	<b>30/07/2020</b>	30/04/2024	9796
9	Bộ Nông nghiệp và Phát triển nông thôn	28/09/2020	<b>23/02/2024</b>	<b>0</b>
10	Bộ Tài chính	15/12/2020	30/04/2024	211722
11	Bộ Tài nguyên và Môi trường	03/10/2020	<b>01/03/2024</b>	<b>0</b>
12	Bộ Thông tin và Truyền thông	11/02/2022	30/04/2024	49202
13	Bộ Tư pháp	18/03/2023	30/04/2024	1003300
<b>14</b>	<b>Bộ Văn hóa, Thể thao và Du lịch</b>	<b>20/06/2020</b>	<b>19/03/2024</b>	<b>0</b>
15	Bộ Xây Dựng	23/07/2020	15/04/2024	4
<b>16</b>	<b>Bộ Y tế</b>	<b>17/07/2020</b>	<b>14/08/2020</b>	<b>0</b>

17	Ngân hàng Nhà nước Việt Nam	02/07/2020	30/04/2024	37140476
<b>18</b>	<b>Thanh tra Chính phủ</b>	<b>10/11/2020</b>	<b>01/10/2023</b>	<b>0</b>
<b>19</b>	<b>Ủy ban Dân tộc</b>	<b>08/10/2020</b>	30/04/2024	1468
<b>20</b>	<b>Văn phòng Chính phủ</b>	<b>22/09/2020</b>	<b>06/10/2022</b>	<b>0</b>
<b>21</b>	Bảo Hiểm Xã Hội	08/11/2020	30/04/2024	114
22	Đài Truyền hình Việt Nam	14/09/2020	30/04/2024	2917
<b>23</b>	<b>Viện Hàn Lâm KHCN</b>	<b>22/09/2020</b>	<b>12/03/2024</b>	<b>0</b>
24	Kiểm toán Nhà nước Việt Nam	09/03/2021	30/04/2024	1130

## 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 30/04/2024)	Số lượng cảnh báo trong tháng 04/2024
1	An Giang	30/09/2020	30/04/2024	911
2	Bắc Giang	21/08/2020	30/04/2024	13127
3	Bắc Kạn	01/09/2020	30/04/2024	9808
<b>4</b>	<b>Bạc Liêu</b>	<b>09/10/2020</b>	<b>19/07/2023</b>	<b>0</b>
5	Bắc Ninh	23/07/2020	30/04/2024	42398
6	Bà Rịa - Vũng Tàu	20/07/2020	30/04/2024	4860
7	Bến Tre	10/08/2020	30/04/2024	17353
8	Bình Định	05/06/2020	30/04/2024	1126
9	Bình Dương	24/04/2020	30/04/2024	381400
10	Bình Phước	23/04/2020	19/04/2024	26895
11	Bình Thuận	31/08/2020	30/04/2024	25664
12	Cà Mau	15/05/2020	30/04/2024	564
13	Cần Thơ	13/04/2020	30/04/2024	4951
14	Cao Bằng	14/08/2020	30/04/2024	3364
15	Đắk Lắk	17/06/2020	30/04/2024	7054
16	Đắk Nông	31/08/2020	30/04/2024	13514
17	Đà Nẵng	09/06/2020	26/04/2024	158
18	Điện Biên	02/06/2020	30/04/2024	27597
19	Đồng Nai	15/06/2020	<b>27/02/2024</b>	<b>0</b>
20	Đồng Tháp	14/07/2020	30/04/2024	780
21	Gia Lai	14/09/2020	30/04/2024	2287
22	Hà Giang	18/08/2020	30/04/2024	1004
<b>23</b>	<b>Hải Dương</b>	<b>04/09/2020</b>	<b>12/05/2022</b>	<b>0</b>
24	Hải Phòng	28/07/2020	26/04/2024	8
25	Hà Nam	22/09/2020	30/04/2024	1775
26	Hà Nội	30/06/2020	29/04/2024	27

27	Hà Tĩnh	06/10/2020	24/04/2024	294
28	Hòa Bình	13/05/2020	30/04/2024	864
29	Hồ Chí Minh	26/06/2020	30/04/2024	8830
30	Hậu Giang	02/10/2020	<b>11/02/2024</b>	<b>0</b>
31	Hưng Yên	22/05/2020	30/04/2024	5287
32	Khánh Hòa	21/09/2020	30/04/2024	80
33	Kiên Giang	24/09/2020	30/04/2024	11039
34	Kon Tum	28/09/2020	30/04/2024	574
35	Lai Châu	26/09/2020	<b>03/02/2024</b>	<b>0</b>
36	Lâm Đồng	22/10/2020	16/04/2024	144
37	Lạng Sơn	08/10/2020	30/04/2024	477
38	Lào Cai	09/07/2020	30/04/2024	256066
39	Long An	22/07/2020	30/04/2024	13838
40	Nam Định	21/09/2020	30/04/2024	2643
41	Nghệ An	09/09/2020	30/04/2024	2501
42	Ninh Bình	28/07/2020	30/04/2024	2652
43	Ninh Thuận	01/09/2020	30/04/2024	79330
<b>44</b>	<b>Phú Thọ</b>	<b>01/10/2020</b>	<b>04/07/2023</b>	<b>0</b>
45	Phú Yên	30/11/2020	30/04/2024	17895
46	Quảng Bình	01/07/2020	30/04/2024	9430
<b>47</b>	<b>Quảng Nam</b>	<b>14/09/2020</b>	<b>31/01/2024</b>	<b>0</b>
48	Quảng Ngãi	12/08/2020	30/04/2024	12377
<b>49</b>	<b>Quảng Ninh</b>	<b>12/09/2020</b>	<b>18/11/2023</b>	<b>0</b>
50	Quảng Trị	24/12/2020	30/04/2024	45032
51	Sóc Trăng	12/08/2020	30/04/2024	59476
52	Sơn La	13/07/2020	30/04/2024	3070
53	Tây Ninh	08/07/2020	30/04/2024	446
54	Thái Bình	25/06/2020	<b>29/03/2024</b>	<b>0</b>
<b>55</b>	<b>Thái Nguyên</b>	<b>19/11/2020</b>	19/04/2024	11492
56	Thanh Hóa	29/09/2020	30/04/2024	405865
57	Thừa Thiên Huế	29/07/2020	30/04/2024	40069

58	Tiền Giang	24/09/2020	30/04/2024	462
59	Trà Vinh	29/07/2020	30/04/2024	116350
60	Tuyên Quang	19/11/2020	<b>29/03/2024</b>	<b>0</b>
61	Vĩnh Long	25/06/2020	30/04/2024	9697
<b>62</b>	<b>Vĩnh Phúc</b>	<b>30/06/2020</b>	23/04/2024	2698
63	Yên Bái	26/08/2020	30/04/2024	3915