UBND TỈNH THÁI NGUYÊN
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

Số: 3829 /STTTT-CNTT
V/v tình hình an toàn thông tin mạng Việt Nam tháng 11/2024 và kết quả giám sát an toàn thông tin mạng tỉnh Thái Nguyên tháng 12/2024

Thái Nguyên, ngày 25 tháng 12 năm 2024

Kính gửi:
- Các sở, ban, ngành, đoàn thể thuộc tỉnh;
- Ủy ban nhân dân các huyện, thành phố;
- Trung tâm Công nghệ thông tin và Truyền thông;
- Các doanh nghiệp: VNPT Thái Nguyên, Viettel Thái Nguyên, Mobifone Thái nguyên.

Sở Thông tin và Truyền thông nhận được Báo cáo số 24/BC-CATTT ngày 16/12/2024 về tình hình an toàn thông tin mạng Việt Nam tháng 11/2024, thực hiện chức năng quản lý nhà nước và tổ chức thực thi pháp luật về an toàn thông tin mạng; Sở Thông tin và Truyền thông thông tin đến các cơ quan, tổ chức, đơn vị về tình hình an toàn thông tin mạng Việt Nam tháng 11/2024, kết quả giám sát an toàn thông tin mạng (SOC) tỉnh Thái Nguyên tháng 12/2024.

Nội dung nhằm 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… để giúp các cơ quan, tổ chức, đơn vị nắm bắt kịp thời các vấn đề an toàn thông tin mạng đang diễn ra, từ đó 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, đơn vị mình.

Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin của các cơ quan, tổ chức, đơn vị, góp phần đảm bảo an toàn cho các hệ thống thông tin dùng chung, liên thông của tỉnh; Sở Thông tin và Truyền thông đề nghị các cơ quan, tổ chức, đơn vị triển khai nội dung sau:

1. Các cơ quan, tổ chức, đơn vị nghiên cứu các nguy cơ, rủi ro về an toàn thông tin theo nội dung khuyến nghị được nêu tại Báo cáo số 24/BC-CATTT và Văn bản này, thực hiện rà soát, đánh giá, xử lý các vấn đề về an toàn thông tin mạng (nếu có).

2. Đề nghị Trung tâm Công nghệ thông tin và Truyền thông, theo chức năng, nhiệm vụ được giao, nghiên cứu nội dung được nêu tại mục 1 Văn bản này, thực hiện rà soát, đánh giá đối với các hệ thống thông tin dùng chung của tỉnh thuộc phạm vi quản lý, xử lý các vấn đề về an toàn thông tin mạng (nếu có) và gửi kết quả báo cáo rà soát về địa chỉ thư điện tử ncsc@ais.gov.vn **chậm nhất trước ngày 28/12/2024.**

Sở Thông tin và Truyên thông đề nghị các cơ quan, tổ chức, đơn vị quan tâm, triển khai thực hiện. Trong quá trình thực hiện nếu có khó khăn, vướng mắc, phản ánh kịp thời về Sở Thông tin và Truyên thông để được hướng dẫn, hỗ trợ. Thông tin đầu mối liên hệ: ông Nguyễn Quang Huy, phòng Công nghệ thông tin, điện thoại 0915373585./.

Nơi nhận:
- Như trên;
- UBND tỉnh (báo cáo);
- Ban Giám đốc;
- Lưu: VT, CNTT.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HÒA X.H.C.N VIỆT NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
TỈNH THÁI NGUYÊN

Đào Ngọc Tuất

PHỤ LỤC: TÌNH AN TOÀN THÔNG TIN,
KẾT QUẢ GIÁM SÁT AN TOÀN THÔNG TIN (SOC)
TỈNH THÁI NGUYÊN

(Kèm theo Công văn số 3829/STTTT-CNTT ngày 25 /12/2024 của Sở Thông tin và Truyền thông)

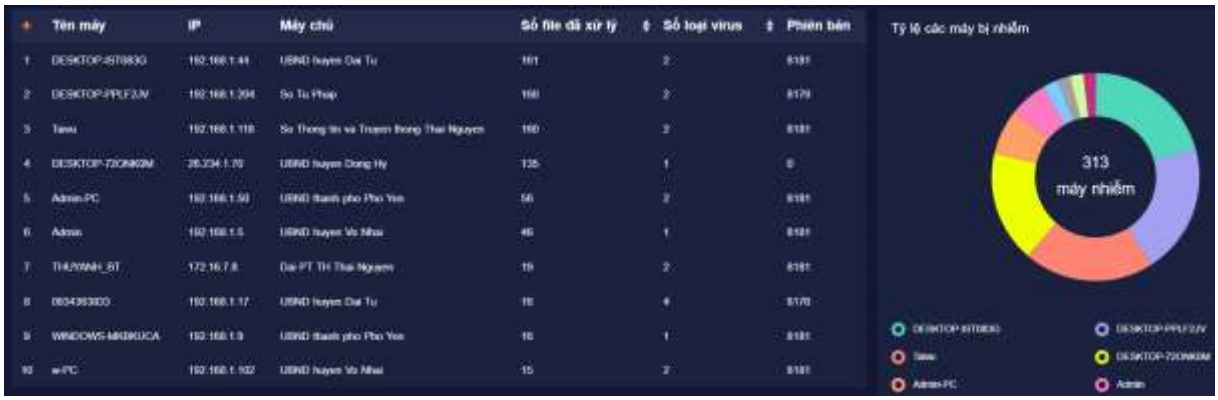
I. KẾT QUẢ GIÁM SÁT AN TOÀN THÔNG TIN MẠNG (SOC) TỈNH THÁI NGUYÊN THÁNG 12/2024

1. Tình hình triển khai công tác phòng chống phần mềm độc hại và chia sẻ dữ liệu mã độc

Đến thời điểm tháng 12/2024, Hệ thống giám sát an toàn thông tin mạng ghi nhận **2.969** máy tính của các cơ quan tổ chức nhà nước được cài đặt và chia sẻ dữ liệu mã độc.

2. Tình hình lây nhiễm mã độc

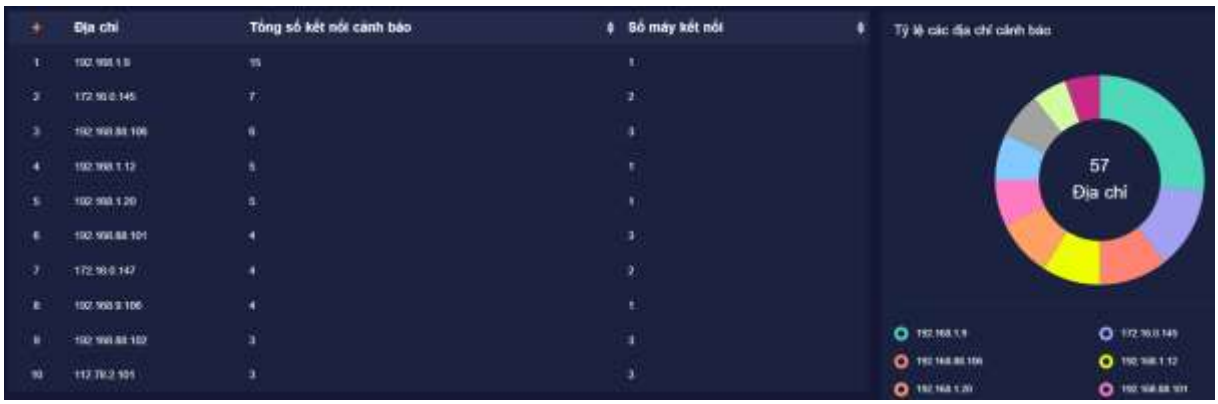
Trong tháng 12/2024, Hệ thống giám sát an toàn thông tin mạng ghi nhận và xử lý 313 máy tính của các cơ quan tổ chức nhà nước có dấu hiệu bị nhiễm mã độc.



(Thống kê danh sách 10 mẫu virus lây nhiều nhất)

3. Kết nối nguy hiểm đã xử lý:

Trong tháng 12/2024, Hệ thống giám sát an toàn thông tin mạng phân tích và phát hiện một số máy tính của cơ quan nhà nước có kết nối đến địa chỉ IP/Domain nghi ngờ độc hại **(57)** do phần mềm phòng chống mã độc đã ghi nhận.



(Thống kê danh sách 10 kết nối nghi ngờ phát sinh trong tháng)

4. Điểm yếu, lỗ hổng tồn tại trên máy tính của các cơ quan tổ chức:

Trong tháng 12/2024, Hệ thống giám sát an toàn thông tin mạng đã ghi nhận có **1.075** điểm yếu, lỗ hổng an toàn thông tin trên máy tính của các cơ quan tổ chức nhà nước trên địa bàn tỉnh.

(Thống kê điểm yếu, lỗ hổng xuất hiện nhiều nhất)

5. Giám sát, đảm bảo an toàn an ninh thông tin

Trong tháng 12/2024, đã phát hiện, ngăn chặn hơn 400.000 kết nối nguy hiểm, loại bỏ 10.213 thư rác, chặn và xử lý 84 thư chứa mã độc.

II. TÌNH AN TOÀN THÔNG TIN TRÊN CẢ NƯỚC

(Chi tiết tại áo cáo số 24/BC-CATTT ngày 16/12/2024 của Cục An toàn thông tin gửi kèm theo)

1. Điểm yếu, lỗ hổng tồn tại trên máy tính của các cơ quan, tổ chức, đơn vị trong tháng 11/2024

Trong tháng 11/2024, Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC) phát hiện trên **73.979** 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; phát hiện hơn **1.600** lỗ hổng trên **5.000** 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.

2. Thống kê các lỗ hổng đáng chú ý được ghi nhận trong tháng 11/2024:

TT	Mã điểm yếu/lỗ hổng	Mô tả	Ghi chú
1	CVE-2024-43451	- Điểm CVSS: 6.5 (Cao) - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực hiện tấn công giả mạo (Spoofing) - Ảnh hưởng: Windows - Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế	https://nvd.nist.gov/vuln/detail/CVE-2024-43451
2	CVE-2024-21287	- Điểm CVSS: 7.5 (Cao) - Mô tả: Lỗ hổng cho phép đối tượng tấn công truy cập và thực hiện các hành vi trái phép - Ảnh hưởng: Oracle Agile PLM Framework thuộc Oracle Supply Chain - Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế	https://nvd.nist.gov/vuln/detail/CVE-2024-21287
3	CVE-2024-11680	- Điểm CVSS: Chưa xác định - Mô tả: Lỗ hổng cho phép đối tượng tấn công truy cập và thực hiện các hành vi trái phép - Ảnh hưởng: ProjectSend - Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế	https://nvd.nist.gov/vuln/detail/CVE-2024-11680
4	CVE-2024-0012	- Điểm CVSS: 9.8 (Nghiêm trọng) - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực hiện tấn công leo thang đặc quyền	https://nvd.nist.gov/vuln/detail/CVE-2024-0012

		- Ảnh hưởng: Palo Alto Networks PAN-OS - Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế	
5	CVE-2024-9474	- Điểm CVSS: 7.2 (Cao) - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực hiện tấn công leo thang đặc quyền - Ảnh hưởng: Palo Alto Networks PAN-OS - Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế	https://nvd.nist.gov/vuln/detail/CVE-2024-9474
6	CVE-2024-44308	- Điểm CVSS: 8.8 (Cao) - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã từ xa - Ảnh hưởng: Safari, iOS, iPadOS, macOS, visionOS của Apple - Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế	https://nvd.nist.gov/vuln/detail/CVE-2024-44308
7	CVE-2024-47575	- Điểm CVSS: 9.8 (Nghiêm trọng) - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã từ xa - Ảnh hưởng: FortiManager - Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế	https://nvd.nist.gov/vuln/detail/CVE-2024-47575
8	CVE-2024-44309	- Điểm CVSS: 6.1 (Trung bình) - Mô tả: Lỗ hổng cho phép đối tượng tấn công truy	https://nvd.nist.gov/vuln/detail/CVE-2024-44309

		cập và thực hiện các hành vi trái phép - Ảnh hưởng: Safari, iOS, iPadOS, macOS, visionOS của Apple - Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế	
9	CVE-2024-45519	- Điểm CVSS: 9.8 (Nghiêm trọng) - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã từ xa - Ảnh hưởng: Zimbra Collaboration (ZCS) - Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế	https://nvd.nist.gov/vuln/detail/CVE-2024-45519
10	CVE-2024-9264	- Điểm CVSS: 8.8 (Cao) - Mô tả: Lỗ hổng cho phép đối tượng tấn công khai thác lỗi Command Injection, truy cập và thực hiện các hành vi trái phép. - Ảnh hưởng: Grafana - Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế	https://nvd.nist.gov/vuln/detail/CVE-2024-9264
11	CVE-2023-32428	- Điểm CVSS: 7.8 (Cao) - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực hiện tấn công leo thang đặc quyền - Ảnh hưởng: macOS, tvOS, iOS, iPadOS, watchOS của Apple - Lỗ hổng chưa có mã khai thác và đang bị khai thác trong thực tế	https://nvd.nist.gov/vuln/detail/CVE-2023-32428

12	CVE-2024-47533	- Điểm CVSS: 9.8 (Nghiêm trọng) - Mô tả: Lỗ hổng cho phép đối tượng tấn công truy cập và thực hiện các hành vi trái phép. - Ảnh hưởng: Cobbler trên Linux - Lỗ hổng chưa có mã khai thác và đang bị khai thác trong thực tế	https://nvd.nist.gov/vuln/detail/CVE-2024-47533

3. Một số lỗ hổng vẫn còn tồn tại phổ biến trên các máy của cơ quan, tổ chức ghi nhận trong tháng 11/2024

TT	Mã điểm yếu/ lỗ hổng	SL máy bị ảnh hưởng	Ghi chú
1	CVE-2022-26809	14343	https://nvd.nist.gov/vuln/detail/CVE-2022-26809
2	CVE-2023-21716	6467	https://nvd.nist.gov/vuln/detail/CVE-2023-21716
3	CVE-2024-48618	5143	https://nvd.nist.gov/vuln/detail/CVE-2024-48618
4	CVE-2024-49046	4722	https://nvd.nist.gov/vuln/detail/CVE-2024-49046
5	CVE-2023-40477	2267	https://nvd.nist.gov/vuln/detail/CVE-2024-40477
6	CVE-2024-10827	1531	https://nvd.nist.gov/vuln/detail/CVE-2024-10827
7	CVE-2024-49039	1521	https://nvd.nist.gov/vuln/detail/CVE-2021-49039
8	CVE-2021-40444	1297	https://nvd.nist.gov/vuln/detail/CVE-2024-40444

9	CVE-2024-10488	1277	https://nvd.nist.gov/vuln/detail/ CVE-2024-10488
10	CVE-2023-38831	1197	https://nvd.nist.gov/vuln/detail/ CVE-2021-38831

III. KHUYẾN NGHỊ VÀ HƯỚNG DẪN KHẮC PHỤC

- Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin, đề nghị các cơ quan, đơn vị, địa phương chỉ đạo bộ phận chuyên trách về công nghệ thông tin/an toàn thông tin phối hợp với bộ phận có liên quan thực hiện kiểm tra, rà soát hệ thống, xử lý các vấn đề về an toàn thông tin mạng trong hệ thống, để tránh nguy cơ bị tấn công.

- Tăng cường giám sát và sẵn sàng phương án xử lý khi phát hiện có dấu hiệu bị khai thác, tấn công mạng; đồng thời thường xuyên theo dõi kênh cảnh báo của các cơ quan chức năng và các tổ chức lớn về an toàn thông tin để phát hiện kịp thời các nguy cơ tấn công mạng.

- Tuyên truyền thường xuyên, liên tục tới toàn thể cán bộ, công chức, viên chức, người lao động của cơ quan, đơn vị mình nhằm nâng cao nhận thức và trang bị kỹ năng đảm bảo an toàn thông tin trên không gian mạng.

- Trong trường hợp cần thiết có thể liên hệ đầu mối hỗ trợ:

+ Sở Thông tin và Truyền thông: ông Nguyễn Quang Huy, Chuyên viên phòng Công nghệ thông tin, số điện thoại: 0915.373.585.

+ Đội Ứng cứu sự cố An toàn thông tin trong các cơ quan nhà nước tỉnh Thái Nguyên: ông Phạm Văn Nối, số điện thoại: 0914.300.486

4. Tài liệu tham khảo

https://msrc.microsoft.com/update-guide/
https://www.zerodayinitiative.com/blog/2024/1/9/the-january-2024-security-update-review