UỶ BAN NHÂN DÂN **XÃ THANH ĐỊNH**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 17 /UBND - VHXH	*Thanh Định, ngày 13 tháng 01 năm 2025*
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	

Kính gửi:

- Các ban ngành, đoàn thể xã Thanh Định;
- Các trường học, trạm y tế xã Thanh Định,

Căn cứ Công văn số 477/VHTT-TH ngày 31/12/2024 của Phòng Văn hóa và Thông tin huyện Định Hóa về 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.

Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin của các ban ngành, đoàn thể, trường học, trạm y tế 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 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… góp phần đảm bảo an toàn cho các hệ thống thông tin dùng chung, liên thông của tỉnh. UBND xã Thanh Định thông tin đến các ban ngành, đoàn thể, trường học, trạm y tế 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).

(Có phụ lục thông tin về các lỗ hổng bảo mật và hướng dẫn khắc phục đính kèm)

Căn cứ các nội dung nêu trên, UBND xã Thanh Định đề nghị các ban ngành, đoàn thể, trường học, trạm y tế trên địa bàn xã quan tâm triển khai thực hiện; trong quá trình thực hiện nếu có khó khăn, vướng mắc, phản ánh kịp thời về Phòng Văn hóa và Thông tin để được hướng dẫn, hỗ trợ. Thông tin đầu mối liên hệ: Ông Ngô Nguyên Long, công chức biệt phái Phòng Văn hóa và Thông tin, số điện thoại 0943905333./.

Nơi nhận: - Như trên; - TT Đảng ủy, TT HĐND; - Lãnh đạo UBND; - Lưu: VP, VHXH.	**TM. ỦY BAN NHÂN DÂN** **CHỦ TỊCH** **Phùng Văn Đăng**

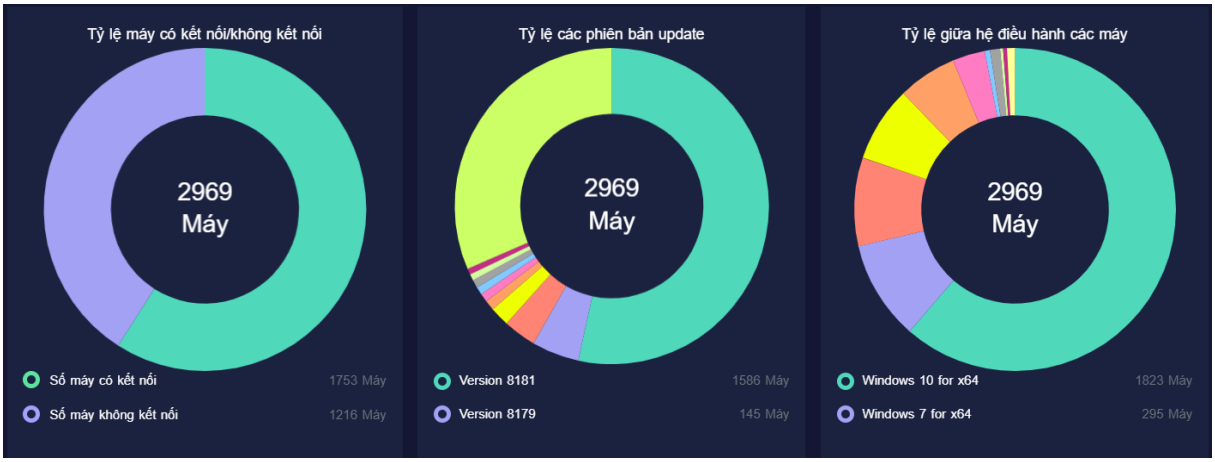
PHỤ LỤC: TÌNH AN TOÀN THÔNG TIN, KẾT QUẢ GIÁM SÁT AN TOÀN THÔNG TIN TẠI TRUNG TÂM (SOC) TỈNH THÁI NGUYÊN

(Kèm theo Công văn số: / VHTT-TT ngày 31 / 12/2024 của Phòng Văn hóa và Thông tin)

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

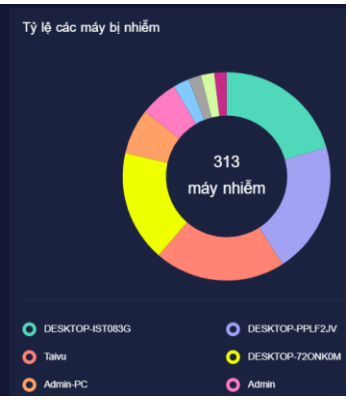
Đến thời điểm tháng 12/2024, Hệ thống giám sát an toàn thông tin mạng ghi nhận **2.969** máy tính của các cơ quan tổ chức nhà nước được cài đặt và chia sẻ dữ liệu mã độc.



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.

	Tên máy	IP	Máy chủ	Số file đã xử lý	Số loại virus	Phiên bản
1	DESKTOP-IST083G	192.168.1.44	UBND huyen Dai Tu	161	2	8181
2	DESKTOP-PPLF2JV	192.168.1.204	So Tu Phap	160	2	8179
3	Taivu	192.168.1.118	So Thong tin va Truyen thong Thai Nguyen	160	2	8181
4	DESKTOP-72ONK0M	26.234.1.70	UBND huyen Dong Hy	135	1	0
5	Admin-PC	192.168.1.50	UBND thanh pho Pho Yen	56	2	8181
6	Admin	192.168.1.5	UBND huyen Vo Nhai	46	1	8181
7	THUYANH_BT	172.16.7.8	Dai PT TH Thai Nguyen	19	2	8181
8	0934363833	192.168.1.17	UBND huyen Dai Tu	16	4	8176
9	WINDOWS-MKBKUCA	192.168.1.9	UBND thanh pho Pho Yen	16	1	8181
10	w-PC	192.168.1.102	UBND huyen Vo Nhai	15	2	8181

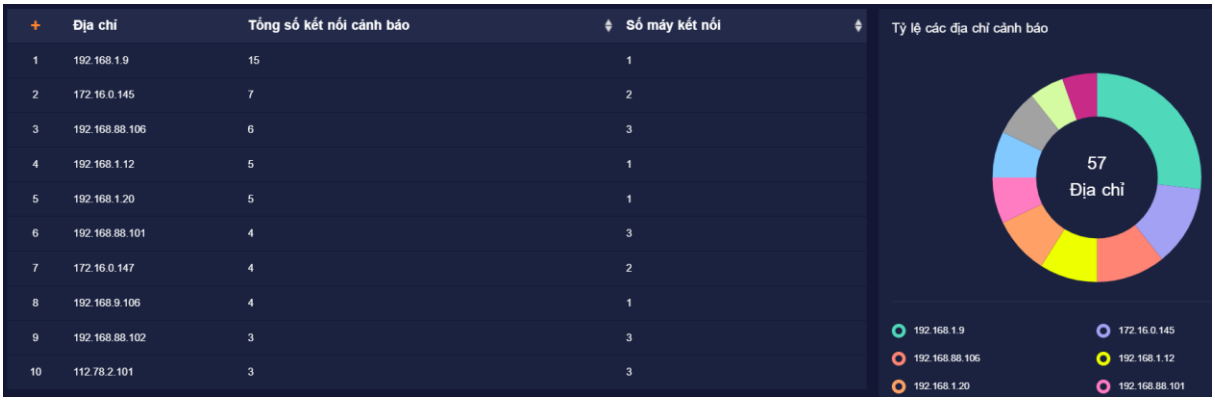


(Thống kê danh sách 10 mẫu virus lây nhiều nhất)

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.



	Địa chỉ	Tổng số kết nối cảnh báo	Số máy kết nối
1	192.168.1.9	15	1
2	172.16.0.145	7	2
3	192.168.88.106	6	3
4	192.168.1.12	5	1
5	192.168.1.20	5	1
6	192.168.88.101	4	3
7	172.16.0.147	4	2
8	192.168.9.106	4	1
9	192.168.88.102	3	3
10	112.78.2.101	3	3

(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.

	Tên lỗ hổng	Số máy có lỗ hổng
1	CVE-2022-26809	791
2	CVE-2021-40444	676
3	CVE-2023-21716	623
4	CVE-2020-0655	390
5	CVE-2020-1097	365
6	CVE-2021-31979	356
7	CVE-2021-1674	313
8	CVE-2022-21907	280
9	CVE-2021-28310	261
10	CVE-2021-1732	253

(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 - 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-2024-0012
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	https://nvd.nist.gov/vuln/detail/CVE-2024-47575

		- Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế	
8	CVE-2024-44309	- Điểm CVSS: 6.1 (Trung bình) - Mô tả: Lỗ hổng cho phép đối tượng tấn công truy 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	https://nvd.nist.gov/vuln/detail/CVE-2024-44309
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	https://nvd.nist.gov/vuln/detail/CVE-2023-32428

		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	
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:

+ Ông Ngô Nguyên Long, công chức biệt phái Phòng Văn hóa và Thông tin, số điện thoại: 0943.905.333.

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

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

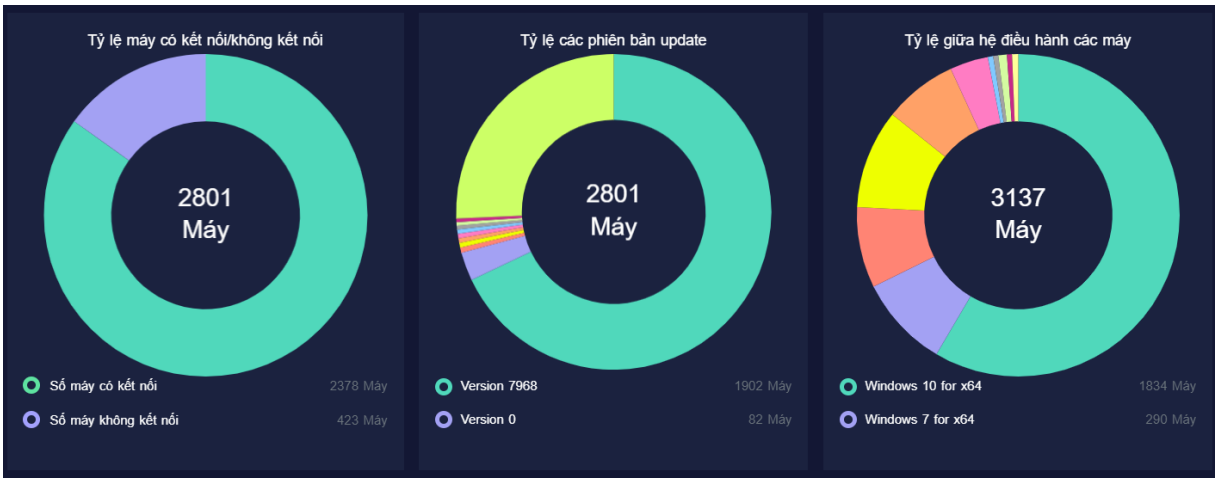
(Kèm theo Công văn số: / VHTT-TT ngày / 8/2024

của Phòng Văn hóa và Thông tin)

I. KẾT QUẢ GIÁM SÁT AN TOÀN THÔNG TIN TẠI TRUNG TÂM GIÁM SÁT AN TOÀN THÔNG TIN MẠNG (SOC) TỈNH THÁI NGUYÊN THÁNG 8/2024

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

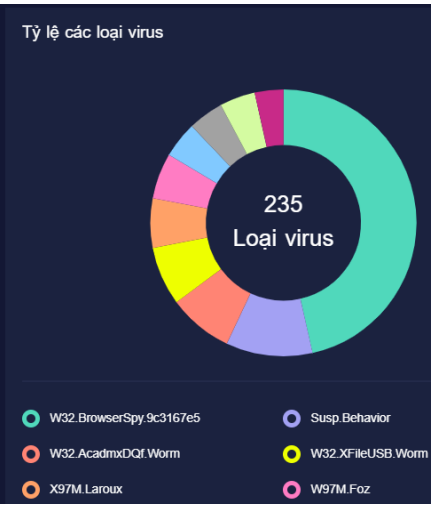
Đến thời điểm ngày 15/8/2024, Hệ thống quản lý tập trung tại Trung tâm SOC tỉnh Thái Nguyên ghi nhận **2.801** máy tính của các cơ quan tổ chức nhà nước được cài đặt và chia sẻ dữ liệu mã độc.



2. Tình hình lây nhiễm mã độc

Trong tháng 8/2024, Hệ thống quản lý tập trung tại Trung tâm SOC tỉnh Thái Nguyên ghi nhận và xử lý 1**65** máy tính của các cơ quan tổ chức nhà nước có dấu hiệu bị nhiễm mã độc.

Loại virus	Số file đã xử lý	Số máy nhiễm	Mức độ nguy hiểm
Adware	561	6	Rất cao
Trojan	127	70	Rất cao
Worm	95	18	Rất cao
Worm	86	57	Rất cao
Trojan	72	26	Rất cao
Trojan	67	18	Rất cao
Worm	53	1	Rất cao
Worm	52	7	Rất cao
Worm	52	2	Rất cao
Worm	42	1	Rất cao

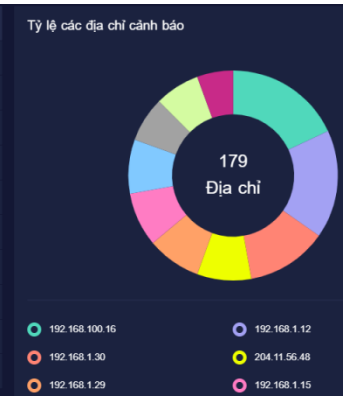


(Thống kê danh sách 10 mẫu virus lây nhiều nhất)

3. Kết nối nguy hiểm đã xử lý:

Trong tháng 8/2024, Hệ thống quản lý tập trung tại Trung tâm SOC tỉnh Thái Nguyên 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 **(179)** do các phần mềm phòng chống mã độc đã ghi nhận.

	Địa chỉ	Tổng số kết nối cảnh báo	Số máy kết nối
1	192.168.100.16	13	1
2	192.168.1.12	12	1
3	192.168.1.30	9	4
4	204.11.56.48	6	5
5	192.168.1.29	6	2
6	192.168.1.15	6	1
7	172.16.5.9	6	1
8	192.168.100.7	5	1
9	192.168.1.32	5	1
10	112.78.2.101	4	4

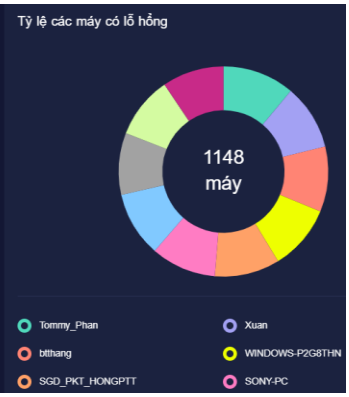


(Thống kê danh sách 10 kết nối nghi ngờ phát sinh trong tháng)

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

Trong tháng 8/2024, Hệ thống quản lý tập trung tại Trung tâm SOC tỉnh Thái Nguyên đã ghi nhận có **1.148** điểm yếu, lỗ hổng an toàn thông tin trên máy tính của các cơ quan tổ chức nhà nước trên địa bàn tỉnh.

	Tên máy	IP	Máy chủ	Tổng số	Phiên bản
1	Tommy_Phan	192.168.88.152	BQL cac Khu cong nghiep	21	7968
2	Xuan	192.168.1.6	So Ngoai Vu	19	7968
3	btthang	10.4.3.107	So TNMT	19	7758
4	WINDOWS-P2G8THN	192.168.0.104	UBND huyen Vo Nhai	19	7968
5	SGD_PKT_HONGPTT	172.16.0.153	So Giao duc va Dao tao	19	7968
6	SONY-PC	192.168.1.104	So TNMT	19	7968
7	Lenovo	192.168.1.17	UBND huyen Phu Binh	19	7968
8	KHANH-HC	192.168.0.104	So Nong nghiep va PTNT	18	7968
9	DungQS	192.168.1.24	UBND huyen Vo Nhai	18	7968
10	Computer	192.168.1.8	UBND huyen Dong Hy	18	7968



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

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

Trong tháng 8/2024, Trung tâm giám sát an toàn thông tin mạng (SOC) tỉnh Thái Nguyên đã **phát hiện** 478.214 kết nối nguy hiểm**, l**oại bỏ 10.549 thư rác, chặn và xử lý 31 thư chứa mã độc.

II. TÌNH AN TOÀN THÔNG TIN TRÊN CẢ NƯỚC

(Chi tiết tại Báo cáo số 13/BC-CATTT ngày 09/8/2024

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 7/2024

Trong tháng 7/2024, Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC) phát hiện trên **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; 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 7/2024:

TT	Mã điểm yếu/lỗ hổng	Mô tả	Ghi chú
1	CVE-2024-6387	- Điểm CVSS: 8.1 (Cao) - Mô tả: Lỗ hổng cho phép đối tượng tấn công truy cập và thực thi các hành vi trái phép. - Ảnh hưởng: OpenSSH. - Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.	https://nvd.nist.gov/vuln/detail/CVE-2024-6387
2	CVE-2024-6327	- Điểm CVSS: 9.8 (Nghiêm trọng) - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Progress Telerik Report Server - Lỗ hổng đang bị khai thác trong thực tế.	https://nvd.nist.gov/vuln/detail/CVE-2024-6327
3	CVE-2023-45249	- Điểm CVSS: 9.8 (Nghiêm trọng) - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Acronis Cyber Infrastructure - Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.	https://nvd.nist.gov/vuln/detail/CVE-2023-45249
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-2024-23692	- Điểm CVSS: 9.8 (Nghiêm trọng) - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Rejetto HTTP File Server - Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.	https://nvd.nist.gov/vuln/detail/CVE-2024-23692
6	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: Windows 10, Windows 11, Windows Server 2008, Windows Server 2012, Windows Server 2016, Windows Server 2019, Windows Server 2022.	https://nvd.nist.gov/vuln/detail/CVE-2024-38112

		- Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.	
7	CVE-2024-37085	- Điểm CVSS: 6.8 (Cao) - Mô tả: Lỗ hổng cho phép đối tượng tấn công truy cập và thực thi các hành vi trái phép. - Ảnh hưởng: VMware ESXi - Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.	https://nvd.nist.gov/vuln/detail/CVE-2024-37085
8	CVE-2024-36991	- 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: Splunk Enterprise trên Windows. - Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.	https://nvd.nist.gov/vuln/detail/CVE-2024-36991
9	CVE-2006-5051	- Điểm CVSS: 8.1 (Cao) - Mô tả: Lỗ hổng cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ, thực thi mã từ xa. - Ảnh hưởng: OpenSSH. - Lỗ hổng đang bị khai thác trong thực tế.	https://nvd.nist.gov/vuln/detail/CVE-2006-5051
10	CVE-2024-20419	- Điểm CVSS: 10.0 (Nghiêm trọng) - Mô tả: Lỗ hổng cho phép đối tượng tấn công truy cập và thực thi các hành vi trái phép. - Ảnh hưởng: Cisco Smart Software Manager On-Prem - Lỗ hổng đang bị khai thác trong thực tế.	https://nvd.nist.gov/vuln/detail/CVE-2024-20419
11	CVE-2024-20401	- Điểm CVSS: 9.8 (Nghiêm trọng) - 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 - Ảnh hưởng: Cisco Secure Email Gateway - Lỗ hổng đang bị khai thác trong thực tế.	https://nvd.nist.gov/vuln/detail/CVE-2024-20401
12	CVE-2024-21412	- Điểm CVSS: 8.1 (Cao) - Mô tả: Lỗ hổng cho phép đối tượng tấn công truy cập và thực thi các hành vi trái phép. - Ảnh hưởng: Windows 10, Windows 11, Windows 2019, Windows 2022. - Lỗ hổng đã có mã khai thác và đang bị khai thác trong thực tế.	https://nvd.nist.gov/vuln/detail/CVE-2024-21412

3. Thông tin các lỗ hổng an toàn thông tin trong các sản phẩm Microsoft công bố tháng 8/2024

STT	CVE	Mô tả	Link tham khảo
1	CVE-2024-38063	- Điểm CVSS: 9.8 (Nghiêm trọng) - Mô tả: Lỗ hổng trong Windows TCP/IP cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows 10, Windows 11, Windows Server 2008, 2012, 2016, 2019, 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38063

2	CVE-2024-38199	- Điểm CVSS: 9.8 (Cao) - Mô tả: Lỗ hổng trong Windows Line Printer Daemon (LPD) Service cho phép đối tượng tấn công thực thi mã từ xa. Thông tin chi tiết về lỗ hổng đã được công bố công khai. - Ảnh hưởng: Windows 10, Windows 11, Windows Server 2008, 2012, 2016, 2019, 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38199
3	CVE-2024-38189	- Điểm CVSS: 8.8 (Cao) - Mô tả: Lỗ hổng trong Microsoft Project cho phép đối tượng tấn công thực thi mã từ xa. Lỗ hổng hiện đang bị khai thác trong thực tế. - Ảnh hưởng: Microsoft Project 2016, Microsoft Office 2019, Microsoft 365 Apps for Enterprise, Microsoft Office LTSC 2021.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38189
4	CVE-2024-38218 CVE-2024-38219	- Điểm CVSS: 8.4 (Cao) - Mô tả: Lỗ hổng trong Microsoft Edge cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Edge (Chromium-based).	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38218 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38219
5	CVE-2024-38193	- Điểm CVSS: 7.8 (Cao) - Mô tả: Lỗ hổng trong Windows Ancillary Function Driver for WinSock cho phép đối tượng tấn công thực hiện leo thang đặc quyền. Lỗ hổng hiện đang bị khai thác trong thực tế. - Ảnh hưởng: Windows 10, Windows 11, Windows Server 2008, 2012, 2016, 2019, 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38193
6	CVE-2024-38107	- Điểm CVSS: 7.8 (Cao) - Mô tả: Lỗ hổng trong Windows Power Dependency Coordinator cho phép đối tượng tấn công thực hiện leo thang đặc quyền. Lỗ hổng hiện đang bị khai thác trong thực tế. - Ảnh hưởng: Windows 10, Windows 11, Windows Server 2012, 2016, 2019, 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38107
7	CVE-2024-38170 CVE-2024-38172	- Điểm CVSS: 7.8 (Cao) - Mô tả: Lỗ hổng trong Microsoft Excel cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft 365 Apps for Enterprise, Microsoft Office LTSC for Mac 2021.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38170 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38172
8	CVE-2024-38171	- Điểm CVSS: 7.8 (Cao) - Mô tả: Lỗ hổng trong Microsoft PowerPoint cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft PowerPoint 2016, Microsoft Office 2019, Microsoft Office LTSC 2021, Microsoft 365 Apps for Enterprise.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38171

9	CVE-2024-38178	- Điểm CVSS: 7.5 (Cao) - Mô tả: Lỗ hổng trong Scripting Engine cho phép đối tượng tấn công thực thi mã từ xa. Lỗ hổng hiện đang bị khai thác trong thực tế. - Ảnh hưởng: Windows 10, Windows 11, Windows Server 2012, 2016, 2019, 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38178
10	CVE-2024-38202	- Điểm CVSS: 7.3 (Cao) - Mô tả: Lỗ hổng trong Windows Update Stack cho phép đối tượng tấn công thực hiện leo thang đặc quyền. Thông tin chi tiết về lỗ hổng đã được công bố công khai. - Ảnh hưởng: Windows 10, Windows 11, Windows Server 2016, 2019, 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38202
11	CVE-2024-38106	- Điểm CVSS: 7.0 (Cao) - Mô tả: Lỗ hổng trong Windows Kernel cho phép đối tượng tấn công thực hiện leo thang đặc quyền. Lỗ hổng hiện đang bị khai thác trong thực tế. - Ảnh hưởng: Windows 10, Windows 11, Windows Server 2012, 2016, 2019, 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38106
12	CVE-2024-21302	- Điểm CVSS: 6.7 (Cao) - Mô tả: Lỗ hổng trong Windows Secure Kernel Mode cho phép đối tượng tấn công thực hiện leo thang đặc quyền. Thông tin chi tiết về lỗ hổng đã được công bố công khai. - Ảnh hưởng: Windows 10, Windows 11, Windows Server 2016, 2019, 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21302
13	CVE-2024-38173	- Điểm CVSS: 6.7 (Cao) - Mô tả: Lỗ hổng trong Microsoft Outlook cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Outlook 2016, Microsoft Office 2019, Microsoft Office LTSC 2021, Microsoft 365 Apps for Enterprise.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38173
14	CVE-2024-38200	- Điểm CVSS: 6.5 (Cao) - Mô tả: Lỗ hổng trong Microsoft Office cho phép đối tượng tấn công thực hiện tấn công giả mạo (spoofing). Thông tin chi tiết về lỗ hổng đã được công bố công khai. - Ảnh hưởng: Microsoft Office 2016, 2019, Microsoft 365 Apps for Enterprise, Microsoft Office LTSC 2021.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38200
15	CVE-2024-38213	- Điểm CVSS: 6.5 (Cao) - Mô tả: Lỗ hổng trong Windows Mark of the Web Security cho phép đối tượng tấn công vượt qua cơ chế bảo vệ. Lỗ hổng hiện đang bị khai thác trong thực tế. - Ảnh hưởng: Windows 10, Windows 11, Windows Server 2012, 2016, 2019, 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38213

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, xác định máy tính

sử dụng hệ điều hành Windows có khả năng bị ảnh hưởng và tiến hành cập nhật bản vá kịp thời cho các lỗ hổng bảo mật nói trên theo hướng dẫn của hãng 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:

+ Ông Ngô Nguyên Long, công chức biệt phái Phòng Văn hóa và Thông tin, số điện thoại: 0943.905.333.

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