UỶ BAN NHÂN DÂN **THỊ TRẤN CHỢ CHU**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 48 /UBND - VHXH V/v tình hình an toàn thông tin và kết quả giám sát an an toàn thông tin tại Trung tâm giám sát ATTT mạng (SOC) tỉnh Thái Nguyên tháng 02/2024	*Chợ Chu, ngày 15 tháng 03 năm 2023*

Kính gửi:

- Các ban ngành, đoàn thể thị trấn Chợ Chu,
- Các trường học, trạm y tế thị trấn Chợ Chu.

Căn cứ Công văn số 42/VHTT-TH ngày 06/3/2024 của Phòng Văn hóa Thông tin huyện Định Hóa về tình hình an toàn thông tin và kết quả giám sát an toàn thông tin tại Trung tâm giám sát ATTT mạng (SOC) tỉnh Thái nguyên tháng 2/2024.

Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin của các cơ quan, đơn vị, góp phần đảm bảo an toàn cho các hệ thống thông tin dùng chung, liên thông của tỉnh; UBND thị trấn Chợ Chu thông tin đến các ban ngành, đoàn thể, trường học, trạm y tế về tình an toàn thông tin tháng 01/2024, kết quả giám sát an toàn thông tin tại Trung tâm giám sát an toàn thông tin mạng (SOC) tỉnh Thái Nguyên tháng 02/2024, khuyến nghị về các lỗ hổng bảo mật có mức ảnh hưởng nghiêm trọng, mức ảnh hưởng cao trong các sản phẩm của hãng Microsoft công bố tháng 02/2024 và hướng dẫn khắc phục.

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

Căn cứ các nội dung nêu trên, UBND thị trấn Chợ Chu đề nghị các ban ngành, đoàn thể, trường học, trạm y tế trên địa bàn thị trấn 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.	**KT. CHỦ TỊCH** **PHÓ CHỦ TỊCH** U.B.N.D THỊ TRẤN CHỢ CHU H.ĐỊNH HÓA T.THÁI NGUYÊN **Nguyễn Trung Kiên**

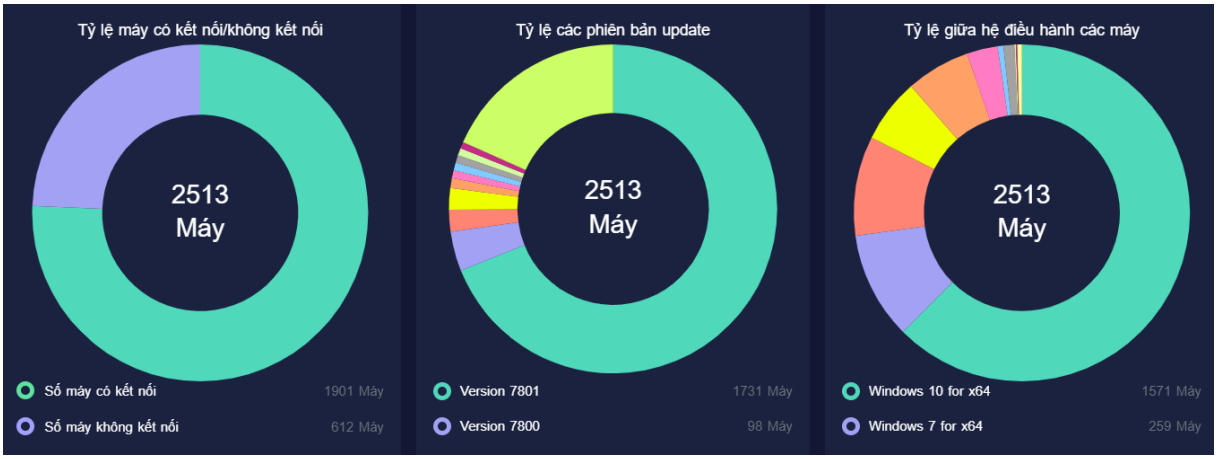
PHỤ LỤC: TÌNH AN TOÀN THÔNG TIN, KẾT QUẢ GIÁM SÁT AN TOÀN THÔNG TIN TẠI TRUNG TÂM (SOC) TỈNH THÁI NGUYÊN

(Kèm theo Công văn số: 42/ VHTT-TT ngày 06/ 3/2024 của Phòng VH&TT)

I. KẾT QUẢ GIÁM SÁT AN TOÀN THÔNG TIN TẠI TRUNG TÂM GIÁM SÁT AN TOÀN THÔNG TIN MẠNG (SOC) TỈNH THÁI NGUYÊN THÁNG 02/2024

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

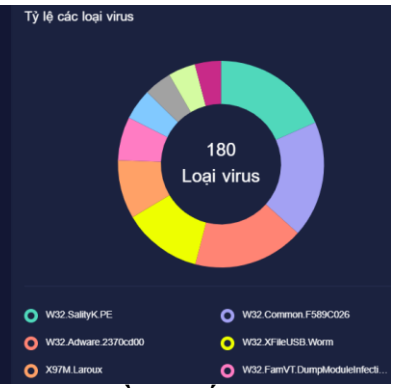
Đến thời điểm ngày 25/02/2024, Hệ thống quản lý tập trung tại Trung tâm SOC tỉnh Thái Nguyên ghi nhận **2.513** máy tính của các cơ quan tổ chức nhà nước được cài đặt và chia sẻ dữ liệu mã độc.



2. Tình hình lây nhiễm mã độc

Trong tháng 02/2024, 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.

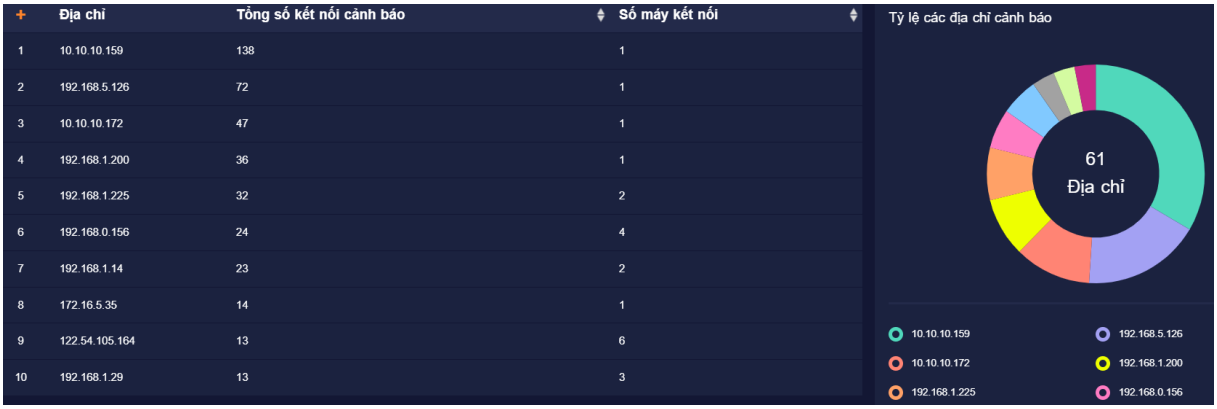
	Tên virus	Loại virus	Số file đã xử lý	Số máy nhiễm	Mức độ nguy hiểm
1	W32.SalityK.PE	PE	224	2	Rất cao
2	W32.Common.F589C026	Virus	222	2	Rất cao
3	W32.Adware.2370cd00	Virus	212	2	Cao
4	W32.XFileUSB.Worm	Worm	151	58	Rất cao
5	X97M.Laroux	Virus	112	14	Rất cao
6	W32.FamVT.DumpModuleInfectiousNME.PE	PE	83	1	Rất cao
7	W97M.Foz	Virus	59	14	Rất cao
8	X97M.NEGS2.Macro	Virus	53	17	Rất cao
9	W32.FakeExeYHPtv.Worm	Worm	52	1	Rất cao
10	W32.DarkKometatgND.PE	PE	50	1	Rất cao



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

3. Kết nối nguy hiểm đã xử lý:

Trong tháng 02/2024, 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 **(61)** do các phần mềm phòng chống mã độc đã ghi nhận.

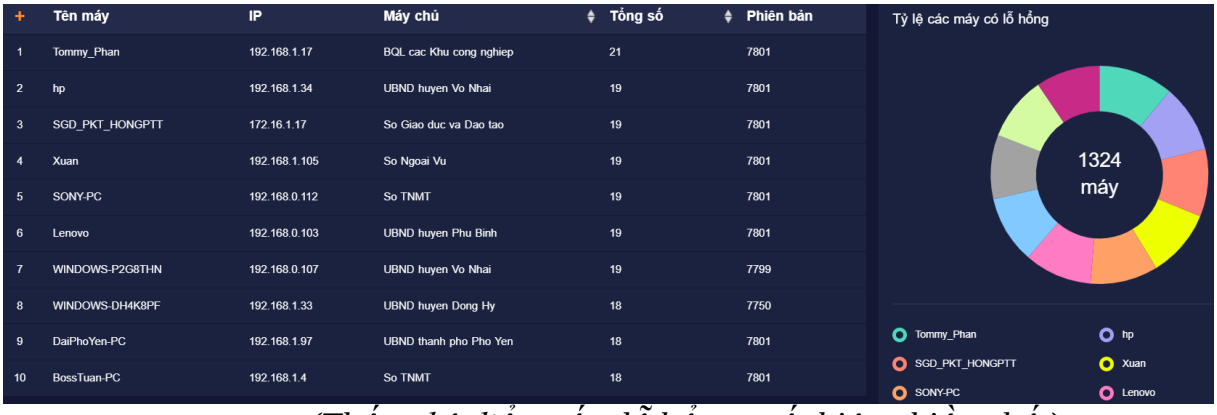


	Địa chỉ	Tổng số kết nối cảnh báo	Số máy kết nối
1	10.10.10.159	138	1
2	192.168.5.126	72	1
3	10.10.10.172	47	1
4	192.168.1.200	36	1
5	192.168.1.225	32	2
6	192.168.0.156	24	4
7	192.168.1.14	23	2
8	172.16.5.35	14	1
9	122.54.105.164	13	6
10	192.168.1.29	13	3

(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 02/2024, Hệ thống quản lý tập trung tại Trung tâm SOC tỉnh Thái Nguyên đã ghi nhận có **1.324** điểm yếu, lỗ hổng an toàn thông tin trên máy tính của các cơ quan tổ chức nhà nước trên địa bàn tỉnh. Một số đơn vị có tỷ lệ máy tính cá nhân tồn tại điểm yếu, lỗ hổng phần mềm cao như: UBND huyện Đồng Hỷ, UBND huyện Võ Nhai, UBND huyện Phú Bình…



	Tên máy	IP	Máy chủ	Tổng số	Phiên bản
1	Tommy_Phan	192.168.1.17	BQL cac Khu cong nghiep	21	7801
2	hp	192.168.1.34	UBND huyen Vo Nhai	19	7801
3	SGD_PKT_HONGPTT	172.16.1.17	So Giao duc va Dao tao	19	7801
4	Xuan	192.168.1.105	So Ngoai Vu	19	7801
5	SONY-PC	192.168.0.112	So TNMT	19	7801
6	Lenovo	192.168.0.103	UBND huyen Phu Binh	19	7801
7	WINDOWS-P2G8THN	192.168.0.107	UBND huyen Vo Nhai	19	7799
8	WINDOWS-DH4K8PF	192.168.1.33	UBND huyen Dong Hy	18	7750
9	DaiPhoYen-PC	192.168.1.97	UBND thanh pho Pho Yen	18	7801
10	BossTuan-PC	192.168.1.4	So TNMT	18	7801

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

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

Trong tháng 02/2024, Trung tâm giám sát an toàn thông tin mạng (SOC) tỉnh Thái Nguyên đã phát hiện 691.120 lượt truy vấn đến hệ hống, ngăn chặn 1.794 lượt truy vấn dò quét trái phép, loại bỏ 14.872 thư rác, chặn và xử lý 30 thư chứa mã độc.

II. TÌNH AN TOÀN THÔNG TIN TRÊN CẢ NƯỚC

(Chi tiết tại Báo cáo số 03/BC-CATTT ngày 27/02/2024 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 01/2024

Trong tháng 01/2024, Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC) phát hiện trên **71.877** điểm yếu, lỗ hổng bảo mật an toàn thông tin tại các hệ thống thông tin của các cơ quan, tổ chức nhà nước, đặc biệt có một số lỗ hổng đã và đang được các nhóm tấn công lợi dụng để thực hiện các cuộc tấn công APT, một số lỗ hổng vẫn còn tồn tại trên nhiều máy của các cơ quan, tổ chức nhà nước chưa được xử lý, cụ thể như sau:

TT	Mã điểm yếu/lỗ hổng	Số lượng máy bị ảnh hưởng	Link tham khảo
1	CVE-2022-26809	**18.411**	https://nvd.nist.gov/vuln/detail/CVE-2022-26809
2	CVE-2024-0814	**9.905**	https://nvd.nist.gov/vuln/detail/CVE-2024-0814
3	CVE-2023-21716	**8.406**	https://nvd.nist.gov/vuln/detail/CVE-2023-21716
4	CVE-2024-0519	**8.301**	https://nvd.nist.gov/vuln/detail/CVE-2024-0519
5	CVE-2022-35737	**5.040**	https://nvd.nist.gov/vuln/detail/CVE-2022-35737

Bên cạnh các điểm yếu/lỗ hổng ghi nhận, Hệ thống kỹ thuật của NCSC còn phân tích và phát hiện nhiều máy tính của cơ quan nhà nước có kết nối đến địa chỉ IP/Domain nghi ngờ độc hại do các phần mềm phòng chống mã độc đã ghi nhận. Thống kê kết nối nghi ngờ phát sinh trong tháng:

STT	IP/Domain nghi ngờ	STT	IP/Domain nghi ngờ
1	differentia[.]ru	2	atomictrivia[.]ru

2. Thông tin các lỗ hổng bảo mật trong các sản phẩm của hãng Microsoft công bố tháng 02/2024

STT	Lỗ hổng bảo mật	Mô tả	Link tham khảo
1	CVE-2024-21410	- Điểm: CVSS: 9.8 (***mức độ ảnh hưởng nghiêm trọng***) - Mô tả: Lỗ hổng trong Microsoft Exchange Server cho phép đối tượng không cần xác thực thực hiện tấn công leo thang đặc quyền. Lỗ hổng hiện đang bị khai thác trong thực tế. - Ảnh hưởng: Microsoft Exchange Server 2016, 2019.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21410
2	CVE-2024-21413 CVE-2024-21378	- Điểm: CVSS: 9.8 (***mức độ ảnh hưởng nghiêm trọng***) - Mô tả: Lỗ hổng trong Microsoft Outlook cho phép đối tượng tấn công không cần xác thực thực thi mã từ xa.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21413 https://msrc.microsoft.com/update-guide/vulnerability/CVE-

STT	Lỗ hổng bảo mật	Mô tả	Link tham khảo
		- Ảnh hưởng: Microsoft Office, Microsoft Office LTSC, Microsoft 365 Apps for Enterprise, Microsoft Outlook.	2024-21378
3	CVE-2024-21399	- Điểm: CVSS: 8.3 ***(mức độ ảnh hưởng trung bình)*** - Mô tả: Lỗ hổng trong Microsoft Edge (Chromium-based) 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-2024-21399
4	CVE-2024-21412	- Điểm: CVSS: 8.1 ***(mức độ ảnh hưởng cao)*** - Mô tả: Lỗ hổng trong Internet Shortcut Files cho phép đối tượng tấn công vượt qua cơ chế bảo mật. Lỗ hổng hiện đang bị khai thác trong thực tế. - Ảnh hưởng: Windows 10, Windows 11, Windows Server 2019, 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21412
5	CVE-2024-21379	- Điểm: CVSS: 7.8 (Cao) - Mô tả: Lỗ hổng trong Microsoft Word cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Word, Microsoft Office, Microsoft Office LTSC, Microsoft 365 Apps for Enterprise.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21379
6	CVE-2024-21384	- Điểm: CVSS: 7.8 (Cao) - Mô tả: Lỗ hổng trong Microsoft Office OneNote cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Office LTSC, Microsoft 365 Apps for Enterprise.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21384
7	CVE-2024-20673	- Điểm: CVSS: 7.8 (Cao) - Mô tả: Lỗ hổng trong Microsoft Office cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Office LTSC, Microsoft Office, Skype for Business.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20673

STT	Lỗ hổng bảo mật	Mô tả	Link tham khảo
8	CVE-2024-21351	- Điểm: CVSS: 7.6 (Cao) - Mô tả: Lỗ hổng trong Windows SmartScreen cho phép đối tượng tấn công vượt qua cơ chế bảo mật. Lỗ hổng hiện đang bị khai thác trong thực tế. - Ảnh hưởng: Windows 10, Windows 11, Windows Server 2016, 2019, 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21351

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