UỶ BAN NHÂN DÂN **THỊ TRẤN CHỢ CHU**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 209 /UBND - VHXH	
V/v tình hình an toàn thông tin và kết quả giám sát an toàn thông tin tại Trung tâm ATTT mạng (SOC) tỉnh Thái Nguyên tháng 8/2023	*Chợ Chu, ngày 06 tháng 09 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 2316/STTTT-CNTT ngày 24/8/2023 của Sở Thông tin và Truyền thông; Công văn số 198/VHTT-TH ngày 29/8/2023 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 8/2023.

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 7/2023, kết quả giám sát an toàn thông tin tại Trung tâm giám sát an toàn thông tin mạng (SOC) tỉnh Thái Nguyên tháng 8/2023, 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 8/2023 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./.

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

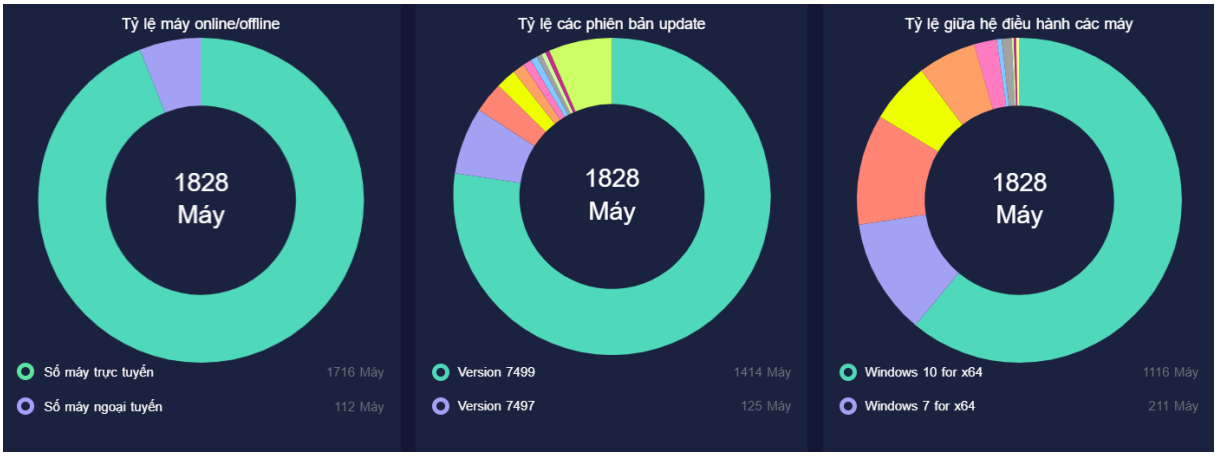
(Kèm theo Công văn số: / VHTT-TT ngày / 8/2023

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 8/2023

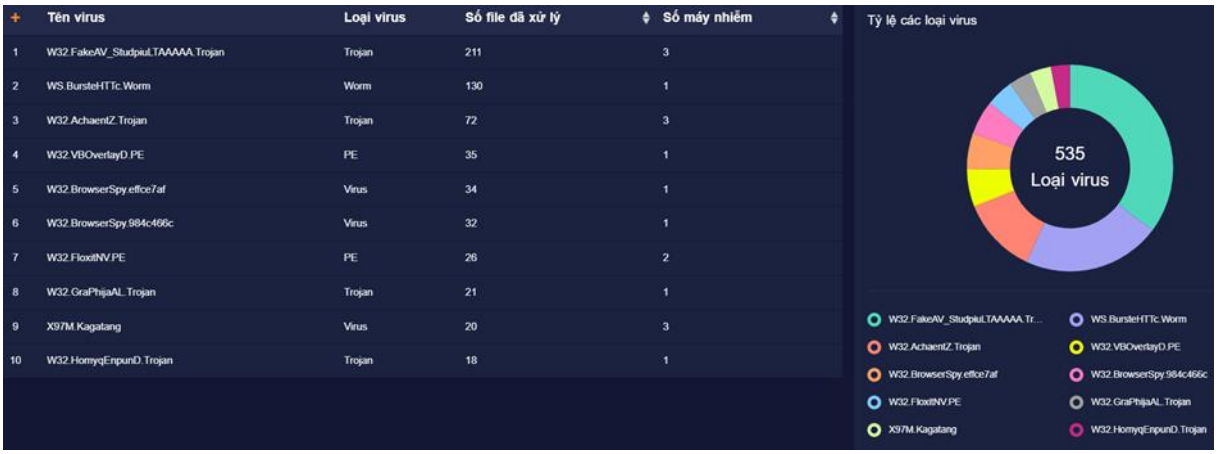
1. Tình hình triển khai công tác phòng chống phần mềm độc hại và chia sẻ dữ liệu mã độc

Đến thời điểm ngày 22/8/2023, Hệ thống quản lý tập trung tại Trung tâm SOC tỉnh Thái Nguyên ghi nhận **1.828** 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 8/2023, Hệ thống quản lý tập trung tại Trung tâm SOC tỉnh Thái Nguyên ghi nhận và xử lý **521** 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
1	W32.FakeAV_StudpiuLTAAAAA.Trojan	Trojan	211	3
2	WS.BursteHTTc.Worm	Worm	130	1
3	W32.AchaentZ.Trojan	Trojan	72	3
4	W32.VBOverlayD.PE	PE	35	1
5	W32.BrowserSpy.effce7af	Virus	34	1
6	W32.BrowserSpy.984c466c	Virus	32	1
7	W32.FloxitNV.PE	PE	26	2
8	W32.GraPhijaAL.Trojan	Trojan	21	1
9	X97M.Kagatang	Virus	20	3
10	W32.HomyqEnpunD.Trojan	Trojan	18	1

(Thống kê Top 10 mẫu virus lây nhiều nhất)

3. Kết nối nguy hiểm đã xử lý:

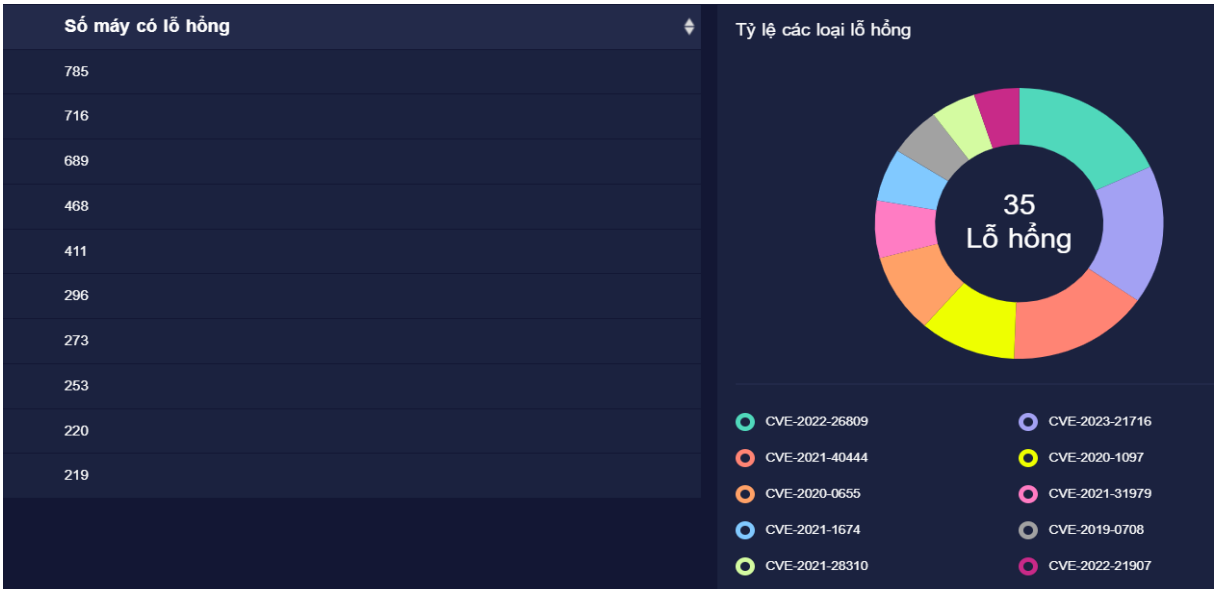
Trong tháng 8/2023, Hệ thống quản lý tập trung tại Trung tâm SOC tỉnh Thái Nguyên phân tích và phát hiện nhiều máy tính của cơ quan nhà nước có kết nối đến địa chỉ IP/Domain nghi ngờ độc hại **(46)** do các phần mềm phòng chống mã độc đã ghi nhận.

+	Địa chỉ	Tổng số kết nối cảnh báo	Số máy kết nối
1	192.168.1.225	22	1
2	disorderstatus.ru	7	1
3	192.168.1.30	6	1
4	184.105.192.2	5	1
5	192.168.3.56	4	2
6	192.168.1.12	4	2
7	a.deltaheavy.ru	4	1
8	192.168.0.103	4	1
9	192.168.2.43	4	1
10	atomictrivia.ru	4	1

(Thống kê TOP 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 8/2023, Hệ thống quản lý tập trung tại Trung tâm SOC tỉnh Thái Nguyên đã ghi nhận có **1.192** 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: Sở Tài nguyên và Môi trường, huyện Định Hóa, huyện Đồng Hỷ, thành phố Phổ Yên, huyện Võ Nhai…



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

5. Giám sát, phát hiện lỗ hổng bảo mật trên các Trang thông tin điện tử (Website) trên địa bàn tỉnh

Trong tháng 8/2023, Trung tâm giám sát an toàn thông tin mạng (SOC) tỉnh Thái Nguyên đã phát hiện và gửi văn bản cảnh báo, khuyến nghị về lỗ hổng bảo mật trên Trang thông tin điện tử (Website) của 04 đơn vị, gồm có: Ban Dân tộc, Sở Nội vụ Báo Văn nghệ Thái Nguyên.

II. TÌNH AN TOÀN THÔNG TIN TRÊN CẢ NƯỚC

(Chi tiết tại Báo cáo số 16/BC-CATTT ngày 21/8/2023 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 7/2023

Trong tháng 7/2023, Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC) phát hiện trên **56.373** 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-2023-3740	**11.193**	https://nvd.nist.gov/vuln/detail/cve-2023-3740
2	CVE-2022-26809	**10.921**	https://nvd.nist.gov/vuln/detail/CVE-2022-26809
3	CVE-2023-3422	**5.375**	https://nvd.nist.gov/vuln/detail/CVE-2023-3422
4	CVE-2023-21716	**4.108**	https://nvd.nist.gov/vuln/detail/CVE-2023-21716
5	CVE-2023-36884	**3.727**	https://nvd.nist.gov/vuln/detail/CVE-2023-36884

2. Thông tin các lỗ hổng bảo mật trong các sản phẩm của hãng Microsoft công bố tháng 8/2023

STT	Lỗ hổng bảo mật	Mô tả	Link tham khảo
1	CVE-2023-21709	- Điểm CVSS: 9.8 ***(mức độ ảnh nghiêm trọng)*** - Mô tả: Lỗ hổng trong Microsoft Exchange Server cho phép đối tượng tấn công	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21709

		thực hiện tấn công nâng cao đặc quyền. - Ảnh hưởng: Exchange Server 2016/2019. - Ảnh hưởng: Microsoft Outlook, Microsoft Office.	
2	CVE-2023-35385 CVE-2023-36910 CVE-2023-36911	- Điểm CVSS: 9.8 ***(mức độ ảnh nghiêm trọng)*** - Mô tả: Lỗ hổng trong Microsoft Message Queuing cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows 10/11, Windows Server.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35385 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36910 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36911
3	CVE-2023-38181	- Điểm CVSS: 8.8 ***(mức độ ảnh hưởng cao)*** - Mô tả: Lỗ hổng trong Microsoft Exchange Server cho phép đối tượng tấn công thực hiện tấn công Spoofing. - Ảnh hưởng: Exchange Server 2016/2019.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38181
4	CVE-2023-29328 CVE-2023-29330	- Điểm CVSS: 8.8 ***(mức độ ảnh hưởng cao)*** - Mô tả: Lỗ hổng trong Microsoft Teams cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Teams dành cho iOS, Mac, Android, Desktop.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29328 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29330
5	CVE-2023-35368 CVE-2023-38185 CVE-2023-35388 CVE-2023-38182	- Điểm CVSS: 8.0/8.8 ***(mức độ ảnh hưởng cao)*** - Mô tả: Lỗ hổng trong Microsoft Exchange Server cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Exchange Server 2016/2019.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35368 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38185 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35388

			https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38182
6	CVE-2023-36895	- Điểm CVSS: 7.8 ***(mức độ ảnh hưởng cao)*** - Mô tả: Lỗ hổng trong Microsoft Outlook cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Office, Microsoft 365 Apps for Enterprise.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36895
7	CVE-2023-36896	- Điểm: CVSS: 7.8 ***(mức độ ảnh hưởng cao)*** - Mô tả: lỗ hổng trong Microsoft Excel cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Excel, Office, Office LTSC, 365 Apps.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36896
8	CVE-2023-35371	- Điểm: CVSS: 7.8 ***(mức độ ảnh hưởng cao)*** - Mô tả: lỗ hổng trong Microsoft Office cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Office, Office LTSC, 365 Apps.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35371

III. KHUYẾN NGHỊ VÀ HƯỚNG DẪN KHẮC PHỤC

- Nhằm đảm bảo an toàn hệ thống, đề nghị bộ phận chuyên trách về công nghệ thông tin/an toàn thông tin tại các cơ quan, đơn vị phối hợp với các 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.

- 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/2023/8/8/the-august-2023-security-update-review