UỶ BAN NHÂN DÂN **THỊ TRẤN CHỢ CHU**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số:255 /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 9/2023	*Chợ Chu, ngày11 tháng 10 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 234/VHTT-TH ngày 29/9/2023 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 9/2023.

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 trên địa bàn thị trấn về tình an toàn thông tin tháng 8/2023, kết quả giám sát an toàn thông tin tại Trung tâm giám sát an toàn thông tin mạng (SOC) tỉnh Thái Nguyên tháng 9/2023, 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 9/2023 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

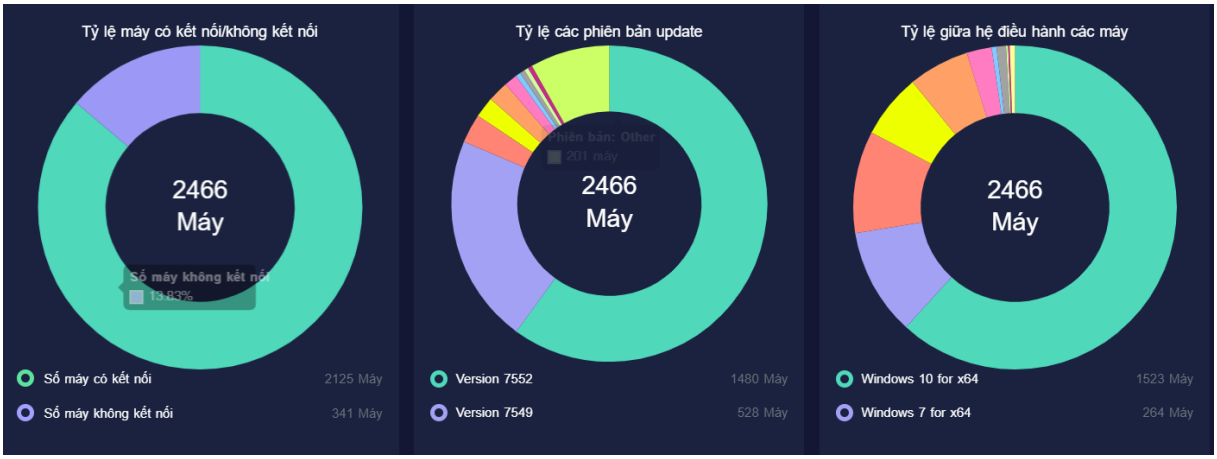
PHỤ LỤC: TÌNH AN TOÀN THÔNG TIN, KẾT QUẢ GIÁM SÁT AN TOÀN THÔNG TIN TẠI TRUNG TÂM (SOC) TỈNH THÁI NGUYÊN

(Kèm theo Công văn số: / VHTT-TT ngày / 9/2023 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 9/2023

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

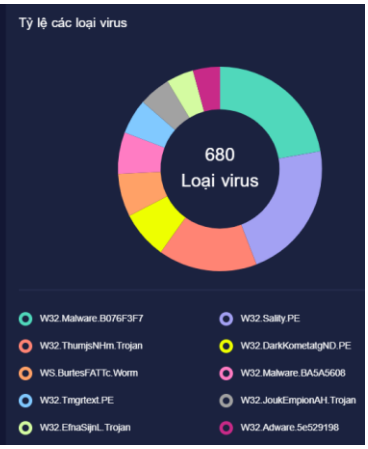
Đến thời điểm ngày 21/9/2023, Hệ thống quản lý tập trung tại Trung tâm SOC tỉnh Thái Nguyên ghi nhận **2.466** máy tính của các cơ quan tổ chức nhà nước được cài đặt và chia sẻ dữ liệu mã độc.



2. Tình hình lây nhiễm mã độc

Trong tháng 9/2023, Hệ thống quản lý tập trung tại Trung tâm SOC tỉnh Thái Nguyên ghi nhận và xử lý **516** 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.Malware.B076F3F7	Virus	88	2
2	W32.Sality.PE	PE	87	8
3	W32.ThumjsNHm.Trojan	Trojan	62	1
4	W32.DarkKometatgND.PE	PE	30	1
5	WS.BurtesFATTc.Worm	Worm	27	1
6	W32.Malware.BA5A5608	Virus	26	1
7	W32.Tmgrtext.PE	PE	22	1
8	W32.JoukEmpionAH.Trojan	Trojan	20	1
9	W32.EfnaSijnL.Trojan	Trojan	17	5
10	W32.Adware.5e529198	Virus	17	3



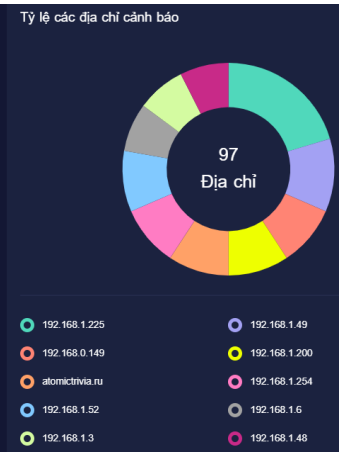
(Thống kê Top 10 mẫu virus lây nhiều nhất)

3. Kết nối nguy hiểm đã xử lý:

Trong tháng 9/2023, 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 **(97)** 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	11	1
2	192.168.1.49	6	1
3	192.168.0.149	5	4
4	192.168.1.200	5	1
5	atomictrivia.ru	5	1
6	192.168.1.254	5	1
7	192.168.1.52	5	1
8	192.168.1.6	4	5
9	192.168.1.3	4	1
10	192.168.1.48	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 9/2023, Hệ thống quản lý tập trung tại Trung tâm SOC tỉnh Thái Nguyên đã ghi nhận có **1.550** 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 Giáo dục và Đào tạo, Sở Tài Nguyên và Môi trường, UBND thành phố Sông Công, UBND huyện Phú Bình…

Số máy có lỗ hổng
1031
949
904
555
538
418
388
328
327
316

(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 9/2023, 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 Sở Nông nghiệp và Phát triển nông thôn (địa chỉ truy cập: https://ntm.thainguyen.gov.vn); ngăn chặn tấn công có chủ đích vào Hệ thống Cơ sở dữ liệu của Liên minh hợp tác xã (địa chỉ truy cập: https://csdllmhtx.thainguyen.gov.vn).

II. TÌNH AN TOÀN THÔNG TIN TRÊN CẢ NƯỚC

(Chi tiết tại Báo cáo số 18/BC-CATTT ngày 21/9/2023 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 8/2023

Trong tháng 8/2023, Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC) phát hiện trên **63.595** 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	**4.840**	https://nvd.nist.gov/vuln/detail/cve-2023-3740
2	CVE-2022-26809	**12.276**	https://nvd.nist.gov/vuln/detail/cve-2022-26809
3	CVE-2023-4078	**6.612**	https://nvd.nist.gov/vuln/detail/CVE-2023-4078
4	CVE-2023-40477	**6.458**	https://nvd.nist.gov/vuln/detail/CVE-2023-40477
5	CVE-2023-4368	**4.987**	https://nvd.nist.gov/vuln/detail/CVE-2023-4368

2. Thông tin các lỗ hổng bảo mật trong các sản phẩm của hãng Microsoft công bố tháng 9/2023

STT	Lỗ hổng bảo mật	Mô tả	Link tham khảo
1	CVE-2023-38146	- Điểm CVSS: 8.8 ***(mức độ ảnh hưởng nghiêm trọng)*** - Mô tả: Lỗ hổng trong Windows Themes cho mã từ xa. - Ảnh hưởng: Windows 10, phép đối tượng tấn công thực thi Windows 11, Windows Server 2019, 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38146
2	CVE-2023-38148	- Điểm: CVSS: 8.8 ***(mức độ ảnh nghiêm trọng)*** - Mô tả: Lỗ hổng trong Internet Connection Sharing (ICS) cho phép đối tượng tấn công không cần xác thực thực thi mã từ xa khi ICS được kích hoạt. - Ảnh hưởng: Windows 10, Windows 11, Windows Server 2022	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38148

3	CVE-2023-36744 CVE-2023-36745 CVE-2023-36756	- Điểm CVSS: 8.0 ***(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: Microsoft Exchange Server.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36744 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36745 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36756
4	CVE-2023-36802	- Điểm CVSS: 7.8 ***(mức độ ảnh hưởng cao)*** - Mô tả: Lỗ hổng trong Streaming Service Proxy cho phép đối tượng tấn công thực hiện leo thang đặc quyền. Lỗ hổng này hiện đang bị khai thác trong thực tế. - Ảnh hưởng: Windows 11.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38181
5	CVE-2023-36792 CVE-2023-36793 CVE-2023-36794 CVE-2023-36796	- Điểm CVSS: 7.8 ***(mức độ ảnh hưởng cao)*** - Mô tả: - Mô tả: Lỗ hổng trong Visual Studio cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft .NET Framework.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36792 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36793 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36794 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36796
6	CVE-2023-29332	- Điểm CVSS: 7.5 ***(mức độ ảnh hưởng cao)*** - Mô tả: Lỗ hổng trong dịch vụ Microsoft Azure Kubernetes Service cho phép đối tượng tấn công không cần xác thực thực hiện tấn công leo thang đặc quyền. - Ảnh hưởng: Microsoft Azure Kubernetes Service.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29332
7	CVE-2023-36761	- Điểm CVSS: 7.8 ***(mức độ ảnh hưởng cao)*** - Mô tả: Lỗ hổng trong Microsoft Word cho phép đối tượng tấn công thu thập thông tin về mã băm NTLM của người dùng. Lỗ hổng này hiện đang bị khai thác trong thực tế. - Ảnh hưởng: Microsoft Word, Microsoft 365.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36761

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.

- Tuyên truyền thường xuyên, liên tục tới toàn thể cán bộ, công chức, viên chức, người lao động của cơ quan, tổ chức, đơn vị mình nhằm nâng cao nhận thức và trang bị kỹ năng an toàn thông tin cho cán bộ, công chức, viên chức 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/2023/9/12/the-september-2023-security-update-review