UBND HUYỆN ĐỊNH HÓA
PHÒNG VĂN HÓA VÀ TT

Số:72 /VHTT-TT

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 03/2024

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập – Tự do – Hạnh phúc

Định Hóa, ngày29 tháng 3 năm 2024

Kính gửi:
- Các cơ quan, ban, ngành, đoàn thể huyện;
- Ủy ban nhân dân các xã, thị trấn;
- Các doanh nghiệp viễn thông trên địa bàn huyện.

Thực hiện Công văn số 623/STTTT-CNTT ngày 27/03/2024 của Sở Thông tin và Truyền thông về tình hình ATTT và kết quả giám sát ATTT tại Trung tâm giám sát ATTT mạng (SOC) tỉnh Thái nguyên tháng 03/2024.

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; Phòng Văn hóa và Thông tin thông tin đến các cơ quan, đơn vị, doanh nghiệp viễn thông, UBND các xã, thị trấn về kết quả giám sát an toàn thông tin tại Trung tâm giám sát an toàn thông tin mạng (SOC) tỉnh Thái Nguyên, 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 03/2024 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, Phòng Văn hóa và Thông tin đề nghị UBND các xã, thị trấn, các cơ quan, đơn vị, doanh nghiệp viễn thông 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;
- Lãnh đạo UBND huyện;
- Lưu: VT, VHTT.

KT. TRƯỞNG PHÒNG
PHÓ TRƯỞNG PHÒNG

PHÒNG VĂN HÓA VÀ THÔNG TIN

Ngô Hoàng

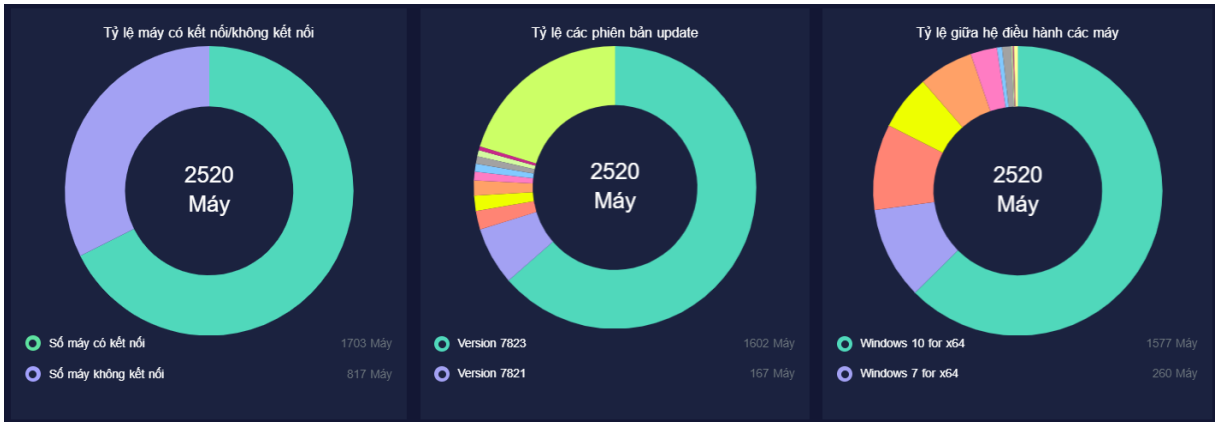
PHỤ LỤC: TÌNH AN TOÀN THÔNG TIN,
KẾT QUẢ GIÁM SÁT AN TOÀN THÔNG TIN TẠI TRUNG TÂM (SOC) TỈNH THÁI NGUYÊN

(Kèm theo Công văn số: / VHTT-TT ngày / 3/2024 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 3/2024

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

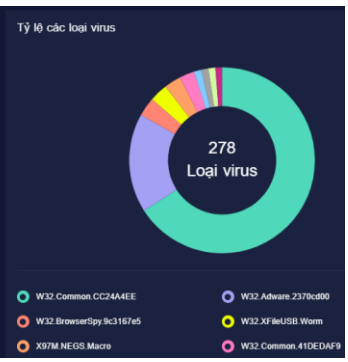
Đến thời điểm ngày 25/3/2024, Hệ thống quản lý tập trung tại Trung tâm SOC tỉnh Thái Nguyên ghi nhận **2.520** máy tính của các cơ quan tổ chức nhà nước được cài đặt và chia sẻ dữ liệu mã độc.



2. Tình hình lây nhiễm mã độc

Trong tháng 3/2024, 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.Common.CC24A4EE	Virus	3302	114	Rất cao
2	W32.Adware.2370cd00	Virus	862	5	Cao
3	W32.BrowserSpy.9c3167e5	Virus	168	2	Rất cao
4	W32.XFileUSB.Worm	Worm	157	57	Rất cao
5	X97M.NEGS.Macro	Virus	147	24	Rất cao
6	W32.Common.41DEDAF9	Virus	131	1	Rất cao
7	W32.Common.1336D90E	Virus	65	51	Rất cao
8	W32.Common.9812EFCE	Virus	62	28	Rất cao
9	X97M.SGV.Macro	Virus	61	17	Rất cao
10	W32.Common.EBD1948B	Virus	57	36	Rất cao



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

3. Kết nối nguy hiểm đã xử lý:

Trong tháng 3/2024, 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 **(292)** do các phần mềm phòng chống mã độc đã ghi nhận.

	Địa chỉ	Tổng số kết nối cảnh báo	Số máy kết nối
1	192.168.168.141	209	1
2	192.168.0.156	36	4
3	10.10.10.159	26	1
4	192.168.1.200	23	1
5	192.168.1.13	20	2
6	10.10.10.172	17	1
7	122.54.105.164	15	7
8	172.16.0.179	12	4
9	172.16.0.110	11	4
10	192.168.1.29	11	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 3/2024, Hệ thống quản lý tập trung tại Trung tâm SOC tỉnh Thái Nguyên đã ghi nhận có **36** 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 thành phố Phổ Yên, UBND huyện Võ Nhai, Sở Giáo dục và Đào tạo…

	Tên lỗ hổng	Số máy có lỗ hổng
1	CVE-2022-26809	874
2	CVE-2023-21716	766
3	CVE-2021-40444	758
4	CVE-2020-0655	439
5	CVE-2020-1097	430
6	CVE-2021-31979	382
7	CVE-2021-1674	345
8	CVE-2022-21907	301
9	CVE-2021-28310	294
10	CVE-2021-1732	283

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

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

Trong tháng 3/2024, Trung tâm giám sát an toàn thông tin mạng (SOC) tỉnh Thái Nguyên đã **phát hiện 682.162 lượt truy vấn đến hệ hống, ngăn chặn 1.257 lượt truy vấn dò quét trái phép, loại bỏ 9.077 thư rác, chặn và xử lý 33 thư chứa mã độc.**

Phối hợp thực hiện rà quét, cảnh báo lỗ hổng bảo mật đối với các hệ thống thông tin: Hệ thống Thư viện số, Phần mềm Sổ tay Đảng viên.

II. 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-2024-21407	- Điểm CVSS: 8.1 (***mức độ ảnh hưởng nghiêm trọng***) - Mô tả: Lỗ hổng trong Windows Hyper-V cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows 10, Windows 11; Windows Server 2012, 2012 R2, 2016, 2019, 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21407
2	CVE-2024-21408	- Điểm CVSS: 5.5 ***(mức độ ảnh hưởng nghiêm trọng)*** - Mô tả: Lỗ hổng trong Windows Hyper-V cho phép đối tượng tấn công thực hiện tấn công từ chối dịch vụ (DoS). - Ảnh hưởng: Windows 10, Windows 11; Windows Server 2016, 2019, 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21408
3	CVE-2024-21334	- Điểm: CVSS: 9.8 ***(mức độ ảnh hưởng cao)*** - Mô tả: Lỗ hổng trong Open Management Infrastructure (OMI) cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: OMI; System Center Operations Manager (SCOM) 2019, 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21334
4	CVE-2024-26198	- Điểm: CVSS: 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: Microsoft Exchange Server 2016, 2019.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-26198

STT	Lỗ hổng bảo mật	Mô tả	Link tham khảo
5	CVE-2024-21411	- Điểm: CVSS: 8.8 ***(mức độ ảnh hưởng cao)*** - Mô tả: Lỗ hổng trong Skype for Consumer cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Skype for Consumer.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21411
6	CVE-2024-21426	- Điểm: CVSS: 7.8 ***(mức độ ảnh hưởng cao)*** - Mô tả: Lỗ hổng trong Microsoft SharePoint Server cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft SharePoint Enterprise Server 2016, Microsoft SharePoint Server 2019; Microsoft SharePoint Server Subscription Edition.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21426

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.

IV. TÀI LIỆU THAM KHẢO

https://msrc.microsoft.com/update-guide/

https://www.zerodayinitiative.com/blog/2024/3/12/the-march-2024-security-update-review