UBND TỈNH THÁI NGUYÊN
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

Số: 187 /STTTT-CNTT
V/v 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 01/2024

CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

Thái Nguyên, ngày 26 tháng 01 năm 2024

Kính gửi:
- Các sở, ban, ngành, đoàn thể thuộc tỉnh;
- Ủy ban nhân dân các huyện, thành phố;
- Trung tâm Công nghệ thông tin và Truyền thông;
- Các doanh nghiệp: VNPT Thái Nguyên, Viettel Thái Nguyên, Mobifone Thái nguyên.

Sở Thông tin và Truyền thông nhận được các Văn bản của Cục An toàn thông tin (Bộ Thông tin và Truyền thông), gồm có: Báo cáo số 01/BC-CATTT ngày 25/01/2024 về tình hình an toàn thông tin tháng 12/2023 và thống kê kết nối chia sẻ dữ liệu về mã độc, giám sát và Công văn số 66/CATTT-NCSC ngày 17/01/2024 về lỗ hổng an toàn thông tin có mức ảnh hưởng nghiêm trọng, mức ảnh hưởng cao trong các sản phẩm của hãng Microsoft công bố tháng 12/2023.

Thực hiện chức năng quản lý nhà nước về an toàn thông tin, 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; Sở Thông tin và Truyền thông thông tin đến các cơ quan, tổ chức, đơn vị về tình an toàn thông tin tháng 12/2023, kết quả giám sát an toàn thông tin tại Trung tâm giám sát an toàn thông tin mạng (SOC) tỉnh Thái Nguyên tháng 01/2024, 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 01/2024 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).*

Sở Thông tin và Truyền thông đề nghị các cơ quan, đơn vị quan tâm, triển khai thực hiện; trong quá trình thực hiện nếu có khó khăn, vướng mắc, phản ánh kịp thời về Sở Thông tin và Truyên thông để được hướng dẫn, hỗ trợ. Thông tin đầu mối liên hệ: Ông Nguyễn Quang Huy, Phòng CNTT, điện thoại 0915373585./.

Nơi nhận:
- Như trên;
- Cục An toàn thông tin (báo cáo);
- UBND tỉnh (báo cáo);
- Ban Giám đốc;
- Lưu: VT, CNTT.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HOÀ X.H.C.N VIỆT NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
TỈNH THÁI NGUYÊN

Đào Ngọc Tuất

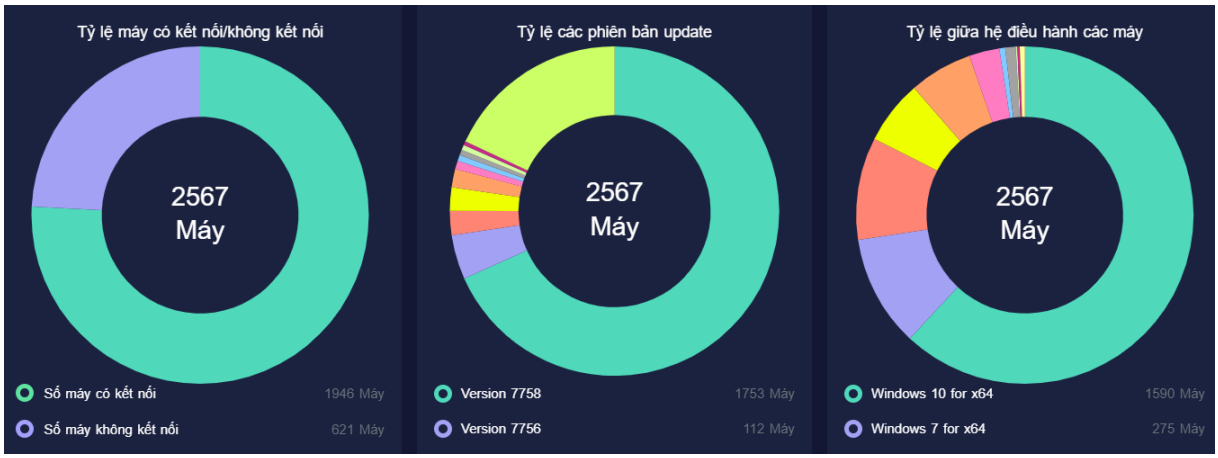
PHỤ LỤC: TÌNH AN TOÀN THÔNG TIN,
KẾT QUẢ GIÁM SÁT AN TOÀN THÔNG TIN TẠI TRUNG TÂM (SOC) TỈNH THÁI NGUYÊN

(Kèm theo Công văn số 187 /STTTT-CNTT ngày 26 /01/2024 của Sở Thông tin và Truyền thông)

I. KẾT QUẢ GIÁM SÁT AN TOÀN THÔNG TIN TẠI TRUNG TÂM GIÁM SÁT AN TOÀN THÔNG TIN MẠNG (SOC) TỈNH THÁI NGUYÊN THÁNG 01/2024

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

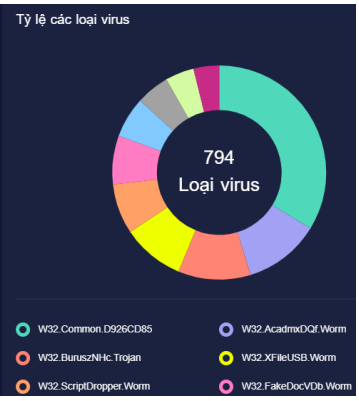
Đến thời điểm ngày 25/01/2024, Hệ thống quản lý tập trung tại Trung tâm SOC tỉnh Thái Nguyên ghi nhận **2.567** máy tính của các cơ quan tổ chức nhà nước được cài đặt và chia sẻ dữ liệu mã độc.



2. Tình hình lây nhiễm mã độc

Trong tháng 01/2024, Hệ thống quản lý tập trung tại Trung tâm SOC tỉnh Thái Nguyên ghi nhận và xử lý **260** 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.D926CD85	Virus	582	1	Rất cao
2	W32.AcadmxDQf.Worm	Worm	199	16	Rất cao
3	W32.BuruszNHc.Trojan	Trojan	189	5	Rất cao
4	W32.XFileUSB.Worm	Worm	162	66	Rất cao
5	W32.ScriptDropper.Worm	Worm	131	1	Rất cao
6	W32.FakeDocVDb.Worm	Worm	127	4	Rất cao
7	X97M.Laroux	Virus	106	20	Rất cao
8	X97M.NEGS2.Macro	Virus	87	9	Rất cao
9	W32.BrowserSpy.9c3167e5	Virus	75	1	Rất cao
10	W32.Common.49DDCF66	Virus	67	2	Rất cao



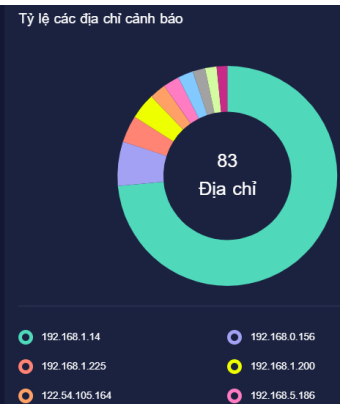
(Thống kê danh sách 10 mẫu virus lây nhiều nhất)

3. Kết nối nguy hiểm đã xử lý:

Trong tháng 01/2024, 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 **(51)** do các phần mềm phòng chống mã độc đã ghi nhận.

	Địa chỉ	Tổng số kết nối cảnh báo	Số máy kết nối
1	192.168.1.14	520	1
2	192.168.0.156	46	4
3	192.168.1.225	28	2
4	192.168.1.200	27	1
5	122.54.105.164	17	7
6	192.168.5.186	17	1
7	192.168.1.59	16	1
8	192.168.1.5	13	1
9	192.168.1.16	12	1
10	172.16.1.32	11	3

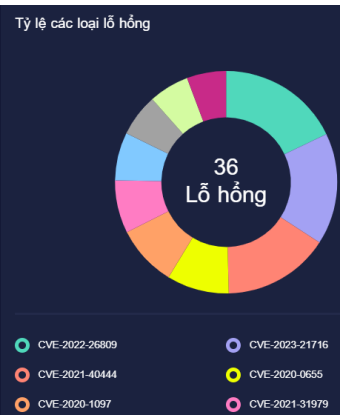


(Thống kê danh sách 10 kết nối nghi ngờ phát sinh trong tháng)

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

Trong tháng 01/2024, Hệ thống quản lý tập trung tại Trung tâm SOC tỉnh Thái Nguyên đã ghi nhận có **1.383** 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 lỗ hổng	Số máy có lỗ hổng
1	CVE-2022-26809	918
2	CVE-2023-21716	832
3	CVE-2021-40444	796
4	CVE-2020-0655	464
5	CVE-2020-1097	457
6	CVE-2021-31979	395
7	CVE-2021-1674	358
8	CVE-2022-21907	316
9	CVE-2021-28310	302
10	CVE-2021-1732	293



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

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

Trong tháng 01/2024, Trung tâm giám sát an toàn thông tin mạng (SOC) tỉnh Thái Nguyên đã phát hiện 969.344 lượt truy vấn đến hệ hống, ngăn chặn 3.411 lượt truy vấn dò quét trái phép, loại bỏ 14.491 thư rác, chặn và xử lý 10 thư chứa mã độc.

6. Giám sát, cảnh báo lỗ hổng bảo mật đối với hệ thống thông tin của các cơ quan nhà nước

Trong tháng 01/2024, Trung tâm giám sát an toàn thông tin mạng (SOC) tỉnh Thái Nguyên đã thực hiện rà quét, cảnh báo lỗ hổng bảo mật đối với các hệ thống thông tin của các cơ quan, đơn vị: Sở Nội vụ (Hệ thống quản lý cán bộ Công chức

viên chức); Sở Tư pháp (Hệ thống CSDL hộ tịch, Phần mềm quản lý CSDL vi bằng; Sở Văn hóa, Thể thao và Du lịch (Hệ thống số hóa bảo tàng); Sở Tài Nguyên và Môi trường (Hệ thống thư viện kho lưu trữ điện tử).

II. TÌNH AN TOÀN THÔNG TIN TRÊN CẢ NƯỚC

(Chi tiết tại Báo cáo số 01/BC-CATTT ngày 25/01/2024 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 12/2023

Trong tháng 12/2023, Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC) phát hiện trên **83.302** 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	**20.405**	https://nvd.nist.gov/vuln/detail/CVE-2022-26809
2	CVE-2023-7024	**12.657**	https://nvd.nist.gov/vuln/detail/CVE-2023-7024
3	CVE-2023-6707	**10.354**	https://nvd.nist.gov/vuln/detail/CVE-2023-6707
4	CVE-2023-21716	**8.890**	https://nvd.nist.gov/vuln/detail/CVE-2023-21716
5	CVE-2023-6512	**8.015**	https://nvd.nist.gov/vuln/detail/CVE-2023-6512

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 TOP 4 kết nối nghi ngờ phát sinh trong tháng:

STT	IP/Domain nghi ngờ	STT	IP/Domain nghi ngờ
1	winnerparagrapdierw[.]fun	3	atomictrivia[.]ru
2	differentia[.]ru	4	disorderstatus[.]ru

2. Thông tin các lỗ hổng bảo mật trong các sản phẩm của hãng Microsoft công bố tháng 01/2024

STT	Lỗ hổng bảo mật	Mô tả	Link tham khảo
1	CVE-2024-20674	- Điểm: CVSS: 9.0 (***mức độ ảnh hưởng nghiêm trọng***) - Mô tả: Lỗ hổng trong Windows Kerberos cho phép đối tượng tấn công vượt qua cơ chế bảo vệ để thực hiện tấn công giả mạo. - Ảnh hưởng: Windows 10, Windows 11; Windows Server 2008, 2012, 2016, 2019, 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20674
2	CVE-2024-21318	- Điểm: CVSS: 8.8 (***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 Server 2016, 2019; Microsoft SharePoint Server Subscription Edition.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21318
3	CVE-2024-20677	- 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 2019; Microsoft Office LTSC; Microsoft 365 Apps.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20677
4	CVE-2024-20700	- Điểm: CVSS: 7.5 ***(mức độ ảnh hưởng cao)*** - Mô tả: Lỗ hổng trong Windows Hyper-V cho phép	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-20700

STT	Lỗ hổng bảo mật	Mô tả	Link tham khảo
		đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows 10, Windows 11; Windows Server 2019, 2022.	

III. KHUYẾN NGHỊ VÀ HƯỚNG DẪN KHẮC PHỤC

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

+ Sở Thông tin và Truyền thông: Ông Nguyễn Quang Huy, Chuyên viên phòng Công nghệ thông tin, số điện thoại: 0915.373.585.

+ Đội Ứng cứu sự cố An toàn thông tin trong các cơ quan nhà nước tỉnh Thái Nguyên: Ông Tạ Tuấn Dũng, Trưởng phòng Quản trị hệ thống và An ninh mạng, Trung tâm Công nghệ thông tin và Truyền thông, Đội phó Đội Ứng cứu sự cố, điện thoại: 0914.300.486

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