UBND TỈNH QUẢNG NGÃI **SỞ THÔNG TIN VÀ TRUYỀN THÔNG**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 2653 /STTTT-BCVT&CNTT	*Quảng Ngãi, ngày 12 tháng 11 năm 2024*

V/v tình hình giám sát an toàn thông tin mạng tập trung của tỉnh trong tháng 10/2024

Kính gửi:

- Ủy ban MTTQ Việt Nam tỉnh;
- Văn phòng: Tỉnh ủy, Đoàn ĐBQH&HĐND, UBND tỉnh;
- Các sở, ban, ngành; Hội, đoàn thể tỉnh;
- UBND các huyện, thị xã, thành phố;
- UBND các xã, phường, thị trấn;
- Báo Quảng Ngãi; Đài Phát thanh và Truyền hình tỉnh.

Thực hiện Chỉ thị số 14/CT-TTg ngày 25/5/2018 của Thủ tướng Chính phủ về việc nâng cao năng lực phòng, chống phần mềm độc hại; Chỉ thị số 09/CT-TTg ngày 23/02/2024 của Thủ tướng Chính phủ về việc tuân thủ quy định pháp luật và tăng cường bảo đảm an toàn hệ thống thông tin theo cấp độ;

Triển khai Kế hoạch số 166/KH-UBND ngày 15/9/2022 của UBND tỉnh về Tăng cường đảm bảo an toàn, an ninh thông tin trong hoạt động các cơ quan nhà nước tỉnh Quảng Ngãi đến năm 2025 và định hướng đến năm 2030;

Sở Thông tin và Truyền thông thông tin về tình hình giám sát An toàn thông tin mạng tập trung của tỉnh trong tháng 10/2024, như sau:

Hệ thống giám sát phòng, chống mã độc tập trung tại Trung tâm dữ liệu tỉnh và 40 cơ quan, đơn vị trong tỉnh. Tính đến ngày 31/10/2024 đã có **4.158 máy trạm** trên địa bàn tỉnh được cài đặt phần mềm phòng chống mã độc tập trung BKAV Endpoint AI và được tự động cập nhật lên phiên bản mới nhất. Hệ thống BKAV Endpoint AI đã phát hiện và xử lý: **12.610** tệp tin chứa mã độc tại: **1.414** máy trạm, tỷ lệ lây nhiễm ~ **34%**.

(*Số liệu chi tiết theo Phụ lục 01 kèm theo Công văn*)

Đối với Hệ thống giám sát tường lửa tập trung tại Trung tâm dữ liệu tỉnh đang kết nối, chia sẻ dữ liệu từ **39** hệ thống thông tin của các đơn vị trong tỉnh và chia sẻ dữ liệu với Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC).

(*Số liệu chi tiết theo Phụ lục 02 kèm theo Công văn*)

Từ ngày 01/10/2024 – 31/10/2024, Hệ thống giám sát, điều hành an toàn, an ninh mạng tập trung (SOC) tại Trung tâm dữ liệu tỉnh Quảng Ngãi đã phát hiện 01 hiết bị máy trạm tại đơn vị trên địa bàn tỉnh có hành vi kết nối đến các IP,máy chủ độc hại, chiếm quyền điều khiển (máy chủ C&C). Sau khi phát hiện, Sở đã cử Trung tâm Chuyển đổi số phối hợp với đơn vị tiến hành khoanh vùng, cô lập và xử lý mã độc nằm trên các máy tính này.

(Số liệu chi tiết theo Phụ lục 03 kèm theo Công văn)

Để tiếp tục nâng cao năng lực phòng, chống phần mềm độc hại trong thời gian đến, giảm thiểu rủi ro mất an toàn thông tin, đồng thời duy trì và nâng cao điểm số chuyển đổi số của tỉnh trong năm 2024 đối với tiêu chí thành phần "An toàn thông tin mạng", đề nghị các đơn vị, địa phương tiếp tục triển khai cài đặt phần mềm phòng, chống mã độc dùng chung của tỉnh là BKAV Endpoint AI hoặc một số phần mềm phòng, chống mã độc khác có thể chia sẻ dữ liệu về NCSC (Ưu tiên phần mềm có bản quyền) nhằm loại bỏ các mã độc tiềm ẩn trong hệ thống; đồng thời rà soát lại số máy không kết nối để kết nối và cập nhật lại phần mềm; kịp thời cử cán bộ phối hợp với Trung tâm Chuyển đổi số để xử lý các sự cố an toàn thông tin mạng liên quan hệ thống của đơn vị. Nhằm tránh tái nhiễm mã độc, khuyến cáo đơn vị nên nâng cấp hệ điều hành Windows 10 trở lên để nhận các cập nhật các bản vá của hệ điều hành, cập nhật các phần mềm bảo mật mới nhất của Microsoft.

Trong quá trình triển khai, nếu cần phân bổ thêm số lượng bản quyền, phát sinh sự cố hoặc cần hỗ trợ kỹ thuật, đề nghị các đơn vị thông báo về Sở Thông tin và Truyền thông để có các biện pháp hỗ trợ, xử lý kịp thời.

Thông tin liên hệ: *Bà Phạm Thị Ngọc Yến, Phó Giám đốc - Trung tâm Chuyển đổi số tỉnh Quảng Ngãi, Sở Thông tin và Truyền thông; Điện thoại: 0906835511; Email: ptnyen-stttt@quangngai.gov.vn*

Đề nghị Thủ trưởng các cơ quan, đơn vị quan tâm chỉ đạo thực hiện./.

Nơi nhận:
- Như trên;
- UBND tỉnh (báo cáo);
- Sở TT&TT: GĐ, các PGĐ, VP;
- Trung tâm CĐS (biết thực hiện);
- Lưu: VT, BCVT&CNTT.

GIÁM ĐỐC

CỘNG HÒA X.H.C.N VIỆT NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
TỈNH QUẢNG NGÃI

Trần Thanh Trường

PHỤ LỤC 01
TÌNH HÌNH SỬ DỤNG PHẦN MỀM PHÒNG CHỐNG MÃ ĐỘC TRÊN ĐỊA BÀN TỈNH QUẢNG NGÃI
(Kèm theo Công văn số 2653/STTTT-BCVT&CNTT ngày 12/11/2024 của Sở Thông tin và Truyền thông tỉnh Quảng Ngãi)

1. Thống kê số lượng file mã độc được xử lý tại các đơn vị

STT	Đơn vị	Số lượng máy trạm đã cài đặt	Số lượng file nghi ngờ mã độc đã được xử lý
I	**Các huyện, thị xã, thành phố**		
1	Thành phố Quảng Ngãi	394	1272
2	Huyện Bình Sơn	234	941
3	Huyện Sơn Tịnh	231	906
4	Thị xã Đức Phổ	186	671
5	Huyện Mộ Đức	258	651
6	Huyện Tư Nghĩa	191	585
7	Huyện Ba Tơ	151	499
8	Huyện Nghĩa Hành	193	327
9	Huyện Trà Bồng	104	218
10	Huyện Sơn Hà	141	177
11	Huyện Minh Long	118	169
12	Huyện Sơn Tây	136	156
13	Huyện Lý Sơn	101	117
II	**Các sở, ban, ngành; Hội đoàn thể tỉnh; Cơ quan khối Đảng**		
14	Sở Kế hoạch và Đầu tư	47	2962
15	Sở Y tế	295	656
16	Sở Giáo dục và Đào tạo	133	360
17	Sở Thông tin và Truyền thông	71	343
18	Cơ quan khối Đảng	220	331
19	BQL ĐTXD DD và CN tỉnh	29	184
20	Sở Nông nghiệp và Phát triển nông thôn	100	171
21	Sở Xây dựng	49	125
22	Sở Tài nguyên và Môi trường	58	93
23	Văn phòng UBND tỉnh	78	83
24	Sở Khoa học và Công nghệ	32	76
25	BQL Khu kinh tế Dung Quất và các KCN	51	70
26	Sở Nội vụ	56	62
27	Sở Tài chính	32	59
28	Ban Quản lý dự án đầu tư xây dựng các công trình giao thông	30	56

STT	Đơn vị	Số lượng máy trạm đã cài đặt	Số lượng file nghi ngờ mã độc đã được xử lý
29	Sở Công Thương	40	55
30	Sở Văn hóa, Thể thao và Du lịch	58	52
31	Ban Dân tộc tỉnh	18	31
32	Sở Lao động - Thương binh và Xã hội	51	28
33	Sở Giao thông vận tải	98	23
34	Tỉnh đoàn Quảng Ngãi	20	19
35	Ủy ban MTTQ VN tỉnh	14	15
36	Đài PTTH tỉnh	28	15
37	Sở Tư pháp	30	13
38	Hội Nông dân tỉnh	16	13
39	Báo Quảng Ngãi	13	11
40	Văn phòng Đoàn ĐBQH&HĐND tỉnh	14	7
41	Hội Liên hiệp Phụ nữ tỉnh	11	6
42	Liên đoàn Lao động tỉnh	12	1
43	Sở Ngoại vụ	16	1
Tổng cộng		**4.158**	**12.610**

2. Thống kê top 20 mã độc lây nhiễm nhiều nhất

STT	Tên mã độc	Loại mã độc	Số file đã xử lý
1	W32.UsbFakeDrive.STC.Worm	Worm	2944
2	X97M.Kangatang.Macro	Macro	1699
3	W32.BrowserSpy.9c3167e5	Adware	1144
4	Susp.Behavior	Trojan	541
5	W32.StuxnetQKE.Trojan	Trojan	424
6	W32.FakeDocVDb.Worm	Worm	398
7	X97M.Laroux	Trojan	397
8	W97M.Foz	Trojan	395
9	X97M.Kagatang	Trojan	304
10	W32.XFileUSB.Worm	Worm	268
11	W32.Common.D2E2A2F3	Trojan	216
12	W32.FakeExeYHPtv.Worm	Worm	151
13	X97M.NEGS2.Macro	Macro	112
14	W32.FamVT.AcaddVM.Worm	Worm	104
15	W32.Common.8943D9E7	Trojan	103
16	W32.Malware.86B71C89	Trojan	102

STT	Tên mã độc	Loại mã độc	Số file đã xử lý
17	W32.BeeyWcsjvulX.Trojan	Trojan	91
18	W32.AcadmxDQf.Worm	Worm	82
19	W32.AcadFSANJPTTc.Worm	Worm	80
20	W32.Common.2A01FC04	Trojan	77

PHỤ LỤC 02
TÌNH HÌNH KẾT NỐI, CHIA SẺ DỮ LIỆU TRÊN HỆ THỐNG GIÁM SÁT TẬP TRUNG TẠI TRUNG TÂM DỮ LIỆU TỈNH
(Kèm theo Công văn số /STTTT-BCVT&CNTT ngày /11/2024 của Sở Thông tin và Truyền thông tỉnh Quảng Ngãi)

Hệ thống giám sát tập trung tại Trung tâm dữ liệu tỉnh đang kết nối, chia sẻ dữ liệu từ **39** hệ thống thông tin của các đơn vị trong tỉnh và chia sẻ dữ liệu với NCSC, cụ thể như sau:

- Sở, ban ngành tỉnh (21 đơn vị): VP UBND tỉnh, Ban Dân tộc, Ban QLKKTDQ và các KCN tỉnh, Thanh tra tỉnh, Sở Kế hoạch và Đầu tư, Sở Văn hoá, Thể thao và Du lịch, Sở Công Thương, Sở Giáo dục và Đào tạo, Sở Giao thông Vận tải, Sở Lao động – Thương binh và Xã hội, Sở Nông nghiệp và PTNT, Sở Nội vụ, Sở Tài chính, Sở Tài nguyên và Môi trường, Sở Tư pháp, Sở Xây dựng, Sở Y tế, Sở Khoa học và Công nghệ, Ban Quản lý dự án đầu tư xây dựng các công trình giao thông tỉnh, Ban QLDA các CT Dân dụng và Công nghiệp tỉnh, Sở Ngoại vụ.

- Huyện, thành phố, thị xã (12 đơn vị): huyện Mộ Đức, huyện Sơn Tịnh, huyện Sơn Tây, huyện Tư Nghĩa, huyện Lý Sơn, huyện Sơn Hà, huyện Nghĩa Hành, thị xã Đức Phổ, huyện Ba Tơ, huyện Bình Sơn, huyện Minh Long, huyện Trà Bồng.

- Các xã, phường, thị trấn (6 đơn vị): thị trấn Mộ Đức, xã Đức Chánh, xã Đức Phong, xã Nghĩa Hoà, xã Nghĩa Trung, thị trấn La Hà.

- Xã Đức Phong - huyện Mộ Đức (Hiện tại bị mất kết nối): Nguyên nhân do thiết bị chập điện và bật nguồn không lên. Đã cử cán bộ phụ trách xuống kiểm tra, thay thế nguồn nhưng thiết bị vẫn không hoạt động.

Lưu ý: Các đơn vị chưa chia sẻ dữ liệu với Hệ thống giám sát tập trung của tỉnh, vui có văn bản ***đề nghị gửi Sở Thông tin và Truyền thông tỉnh Quảng Ngãi để kết nối, chia sẻ*** *(Hệ thống giám sát tập trung của tỉnh hiện có thể kết nối với các hệ thống thông tin có thiết bị tường lửa như: sophos, fortigate, pfsense,...và các dòng thiết bị tường lửa có chức năng* ***Log setting*****).**

PHỤ LỤC 03
BÁO CÁO ỨNG CỨU, KHẮC PHỤC SỰ CỐ MẠNG MÁY TÍNH TẠI CÁC ĐƠN VỊ TRÊN ĐỊA BÀN TỈNH
(Kèm theo Công văn số /STTTT-BCVT&CNTT ngày /11/2024 của Sở Thông tin và Truyền thông tỉnh Quảng Ngãi)

1. Tổng quan

Hệ thống giám sát an toàn thông tin tập trung tại Trung tâm dữ liệu tỉnh: Từ ngày 01/10/2024 – 31/10/2024, hệ thống đã phát hiện 01 thiết bị máy trạm tại các đơn vị trên địa bàn tỉnh có hành vi kết nối đến các IP, máy chủ độc hại, chiếm quyền điều khiển (máy chủ C&C). Qua rà soát, phát hiện máy trạm bị có hành vi thực hiện truy vấn đến IP độc hại để thực thi chiếm quyền và đánh cắp dữ liệu và tiến hành lây lan sang các thiết bị máy trạm khác trên cùng một hệ thống mạng LAN. Sau khi phát hiện, đơn vị đã tiến hành khoanh vùng, cô lập và xử lý mã độc nằm trên các máy tính này.

2. Thống kê chi tiết

2.1. Danh sách các đơn vị bị ảnh hưởng

STT	Đơn vị	Số lượng máy trạm nhiễm mã độc	Số lượng tài khoản bị lộ lọt thông tin	Phạm vi ảnh hưởng
1	Sở Giao thông vận tải	1		Thiết bị máy trạm thuộc hệ thống mạng LAN tại đơn vị

2.2. Thống kê chi tiết các thiết bị kết nối mã độc

STT	Nguồn mã độc
1	Detect query to query tới IOC độc hại IOC malware

3. Kết quả thực hiện

3.1. Danh sách các đơn vị đã thực hiện gỡ bỏ mã độc

STT	Đơn vị	Kênh kết nối/ Hỗ trợ kết nối	Số lượng máy trạm nhiễm mã độc	Số lượng tài khoản bị lộ lọt thông tin	Đã xử lý/Chưa xử lý
1	Sở Giao thông vận tải	Ultraview/ Cán bộ phụ trách CNTT	1		Đã xử lý

4. Khuyến cáo

- Khuyến cáo các đơn vị thực hiện cài đặt đầy đủ phần mềm phòng, chống mã độc dùng chung của tỉnh là BKAV Endpoint AI hoặc một số phần mềm phòng, chống mã độc khác (Ưu tiên phần mềm có bản quyền) nhằm loại bỏ các mã độc tìm ẩn trong hệ thống và cập nhật.

- Các máy trạm bị nhiễm mã độc đang sử dụng hệ điều hành Windows 7 Professional/Ultimate, phiên bản này đã ngừng hỗ trợ bởi Microsoft, do đó bị ảnh hưởng bởi nhiều lỗ hổng từ mức cao đến nghiêm trọng như chiếm quyền điều khiển từ xa, leo thang đặc quyền, từ chối dịch vụ,... Nhằm tránh tái nhiễm mã độc, khuyến cáo đơn vị nên nâng cấp hệ điều hành Windows 10 trở lên để nhận các cập nhật hệ điều hành, cập nhật các phần mềm bảo mật mới nhất của Microsoft về các tính năng bảo mật, các lỗ hổng.

- Khi nhận được cảnh báo từ Hệ thống giám sát, điều hành an toàn, an ninh mạng tập trung (SOC) tại Trung tâm dữ liệu tỉnh Quảng Ngãi về thông tin IP, máy tính người sử dụng đầu cuối nghi ngờ có các hành vi kết nối đến các IP, máy chủ độc hại, chiếm quyền điều khiển (máy chủ C&C), đơn vị chỉ đạo cán bộ phụ trách CNTT tại đơn vị khẩn trương truy tìm các máy tính bị sự cố và cung cấp các thông tin có liên quan gửi về cán bộ kỹ thuật của Trung tâm Chuyển đổi số phối hợp xử lý để đảm bảo an toàn, an ninh thông tin của đơn vị và thực hiện đúng các quy định về các hoạt động điều phối, ứng cứu sự cố an toàn thông tin mạng trên địa bàn tỉnh Quảng Ngãi.
