UBND TỈNH QUẢNG NGÃI
**SỞ THÔNG TIN VÀ TRUYỀN THÔNG**

Số: 925 /STTTT-BCVT&CNTT

V/v tình hình theo dõi trên các hệ thống giám sát tập trung tỉnh Quảng Ngãi tháng 4/2024

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

*Quảng Ngãi, ngày 14 tháng 5 năm 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 đã triển khai giải pháp phòng, chống mã độc tập trung tại Trung tâm dữ liệu tỉnh và cho hơn 40 cơ quan, đơn vị trong tỉnh. Tính đến ngày 30/4/2024 đã có **4.287 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: **26.991** tệp tin chứa mã độc tại: **1.110 máy trạm**, tỷ lệ lây nhiễm ~ **25,90%.**

(*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 38 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 01/4/2024 - 30/4/2024, 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 03 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) và 02 tài khoản lộ lọt dữ liệu trên môi trường mạng. Qua rà soát, máy bị nhiễm dòng mã độc liên quan đến giao thức SMB (Server Message Block), khi một thiết bị bị nhiễm, sẽ liên tục thực hiện scan port 445 đối với các IP cùng dãy mạng, thực hiện khai thác lỗi MS17-010 (hay được biết đến với tên gọi Eternal Blue) để leo ngang

hàng qua các máy khác, và tiến hành khai thác trên các trình duyệt internet để thực hiện khai thác các tài khoản mật khẩu được lưu trên trình duyệt. Sau khi phát hiện, đã 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 (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 Công nghệ thông tin và Truyền thông 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 Công nghệ thông tin và Truyền thông, Sở Thông tin và Truyền thông; điện thoại: 0906835511; Email: ptnyen-stttt@quangngai.gov.vn.*

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

***Nơi nhận:***
- Như trên;
- Sở TT&TT: GĐ, PGĐ;
- Trung tâm CNTT&TT (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: /STTTT-BCVT&CNTT ngày /5/2024 của Sở Thông tin và Truyền thông)*

**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 | Huyện Sơn Hà | 160 | 5645 |
| 2 | Thị xã Đức Phổ | 197 | 2459 |
| 3 | Thành phố Quảng Ngãi | 322 | 1701 |
| 4 | Huyện Mộ Đức | 219 | 1379 |
| 5 | Huyện Tư Nghĩa | 209 | 808 |
| 6 | Huyện Bình Sơn | 267 | 780 |
| 7 | Huyện Sơn Tịnh | 201 | 717 |
| 8 | Huyện Nghĩa Hành | 175 | 666 |
| 9 | Huyện Ba Tơ | 178 | 390 |
| 10 | Huyện Sơn Tây | 169 | 322 |
| 11 | Huyện Lý Sơn | 159 | 289 |
| 12 | Huyện Trà Bồng | 160 | 256 |
| 13 | Huyện Minh Long | 128 | 238 |
| **II** | **Các sở, ban, ngành; Hội đoàn thể tỉnh; Cơ quan khối Đảng** | | |
| 14 | Sở Văn hóa, Thể thao và Du lịch | 57 | 2493 |
| 15 | Sở Tài chính | 51 | 1283 |
| 16 | Sở Tài nguyên và Môi trường | 71 | 1142 |
| 17 | Sở Xây dựng | 52 | 932 |
| 18 | Sở Kế hoạch và Đầu tư | 62 | 757 |
| 19 | BQL Khu kinh tế Dung Quất và các KCN | 35 | 733 |
| 20 | Sở Thông tin và Truyền thông | 67 | 688 |
| 21 | Sở Công Thương | 49 | 590 |
| 22 | Văn phòng UBND tỉnh | 84 | 537 |
| 23 | Sở Nông nghiệp và Phát triển nông thôn | 120 | 367 |
| 24 | Sở Giáo dục và Đào tạo | 143 | 329 |
| 25 | Sở Y tế | 183 | 259 |
| 26 | Ban Quản lý dự án đầu tư xây dựng các công trình giao thông | 33 | 201 |
| 27 | BQL ĐTXD DD và CN tỉnh | 31 | 176 |
| 28 | Sở Nội vụ | 58 | 170 |

| STT | Đơn vị | Số lượng máy trạm đã cài đặt | Số lượng file nghi ngờ mã độc đã được xử lý |
|---|---|---|---|
| 29 | Đài PTTH tỉnh | 27 | 149 |
| 30 | Tỉnh đoàn Quảng Ngãi | 27 | 147 |
| 31 | Sở Khoa học và Công nghệ | 42 | 124 |
| 32 | Sở Lao động - Thương binh và Xã hội | 50 | 117 |
| 33 | Sở Giao thông vận tải | 93 | 45 |
| 34 | Sở Tư pháp | 34 | 33 |
| 35 | Hội Nông dân tỉnh | 17 | 22 |
| 36 | Liên đoàn Lao động tỉnh | 17 | 16 |
| 37 | Ủy ban MTTQ VN tỉnh | 15 | 10 |
| 38 | Hội Liên hiệp Phụ nữ tỉnh | 14 | 8 |
| 39 | Sở Ngoại vụ tỉnh | 15 | 5 |
| 40 | Ban Dân tộc tỉnh | 20 | 4 |
| 41 | Văn phòng Đoàn ĐBQH&HĐND tỉnh | 14 | 3 |
| 42 | Báo Quảng Ngãi | 15 | 1 |
| 43 | Cơ quan khối Đảng | 247 | 0 |
| **Tổng cộng** | | **4.287** | **26.991** |

**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.Common.CC24A4EE | Adware | 4881 |
| 2 | X97M.Kangatang.Macro | Adware | 4248 |
| 3 | W32.Vetor.PE | Adware | 2627 |
| 4 | W32.Malware.B1A47CAC | Adware | 2447 |
| 5 | W32.Malware.552A3D1 | Adware | 924 |
| 6 | W32.Malware.F88139FE | Adware | 711 |
| 7 | W32.UsbFakeDrive.STC.Worm | Adware | 685 |
| 8 | W32.Common.1CC74ED3 | Adware | 675 |
| 9 | W32.Malware.C862E8BB | Adware | 665 |
| 10 | W32.Malware.537380BF | Adware | 554 |
| 11 | W32.RontokbroE.Worm | Adware | 505 |
| 12 | W32.Malware.EB6D615A | Adware | 487 |
| 13 | W97M.Foz | Adware | 438 |
| 14 | W32.AcadFSANJPTTc.Worm | Adware | 418 |
| 15 | W32.GraPhijaAP.Trojan | Adware | 402 |
| 16 | X97M.Laroux | Adware | 391 |

| STT | Tên mã độc | Loại mã độc | Số file đã xử lý |
|---|---|---|---|
| 17 | W32.AcadmxDQf.Worm | Adware | 376 |
| 18 | W32.Adware.2370cd00 | Adware | 373 |
| 19 | W32.Malware.43A88D98 | Adware | 368 |
| 20 | W32.BrowserSpy.9c3167e5 | Adware | 322 |

**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 /5/2024 của Sở Thông tin và Truyền thông)*

Hệ thống giám sát tập trung tại Trung tâm dữ liệu tỉnh đang kết nối, chia sẻ dữ liệu từ 38 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 (11 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.

- 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.

- Có 1 đơn vị có thiết bị chưa chia sẻ dữ liệu với hệ thống giám sát tập trung. Để thực hiện kết nối, các đơn vị cần cho phép thực hiện kết nối từ xa và Trung tâm sẽ cử chuyên viên trực tiếp đến đơn vị (nếu không kết nối từ xa) để thực hiện cấu hình là:

- Huyện Trà Bồng (Đã kết nối trong năm 2023, hiện bị mất kết nối). Nguyên nhân do không thể kết nối đăng nhập từ xa hoặc tường lửa bị sự cố.

**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 /5/2024 của Sở Thông tin và Truyền thông)*

## 1. Tổng quan

Hệ thống giám sát an toàn thông tin tập trung tại Trung tâm dữ liệu tỉnh: Từ ngày 01/4/2024 - 30/4/2024, hệ thống đã phát hiện 03 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) và 02 tài khoản lộ lọt thông tin trên môi trường mạng. Qua rà soát, máy bị nhiễm dòng mã độc liên quan đến giao thức SMB (Server Message Block), khi một thiết bị bị nhiễm, sẽ liên tục thực hiện scan port 445 đối với các IP cùng dãy mạng, thực hiện khai thác lỗi MS17-010 (hay được biết đến với tên gọi Eternal Blue) để leo ngang hàng qua các máy khác, và tiến hành khai thác trên các trình duyệt internet để thực hiện khai thác các tài khoản mật khẩu được lưu trên trình duyệt. 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 Xây dựng | 1 | | Thiết bị máy trạm thuộc hệ thống mạng LAN tại đơn vị |
| 2 | Sở Văn hóa, Thể thao và Du lịch | 1 | | Thiết bị máy trạm thuộc hệ thống mạng LAN tại đơn vị |
| 3 | Sở Tài nguyên và Môi trường | 1 | | Thiết bị máy trạm thuộc hệ thống mạng LAN tại đơn vị |
| 4 | Huyện Ba Tơ | | 2 | Tài khoản hệ thống quản lý văn bản và điều hành |

### 2.2. Thống kê chi tiết các thiết bị kết nối mã độc C&C Server

| STT | Nguồn mã độc |
|---|---|
| 1 | Detect query to 192.243.61.227 IOC of ApateWeb malware |
| 2 | Detect query to 185.220.101.48 IOC of Log4j_Scan malware |
| 3 | Detect query to 51.15.58.224 IOC of coinminer malware |
| 4 | Lộ lọt tài khoản office.quangngai.gov.vn trên hệ thống giám sát an ninh mạng |

**3. Kết quả thực hiện**

**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 Xây dựng | Ultraview/ Cán bộ phụ trách CNTT | 1 | | Đã xử lý |
| 2 | Sở Văn hóa, Thể thao và Du lịch | Ultraview/ Cán bộ phụ trách CNTT | 1 | | Chưa xử lý (Cán bộ phụ trách CNTT chưa tìm được IP: 10.0.0.224 thực hiện kết nối độc hại) |
| 3 | Sở Tài nguyên và Môi trường | Ultraview/ Cán bộ phụ trách CNTT | 1 | | Đã xử lý |
| 4 | Huyện Ba Tơ | Cán bộ phụ trách CNTT | | 2 | 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), đề nghị 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 Công nghệ thông tin và Truyền thông 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./.

---