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: 1283 /TB-STTTT

Quảng Ngãi, ngày 12 tháng 12 năm 2019

THÔNG BÁO
Về việc: Mời học viên tham gia "Diễn tập ứng cứu, phòng chống sự cố về an toàn thông tin năm 2019"

Kính gửi: …….....

Thực hiện chức năng quản lý nhà nước về CNTT và chương trình công tác năm 2019, nhằm tiếp tục tập huấn nâng cao nhận thức và kỹ năng quản lý nhà nước về ứng cứu, phòng chống sự cố về an toàn thông tin, Sở Thông tin và Truyền thông phối hợp với các đơn vị có liên quan tổ chức "Diễn tập ứng cứu, phòng chống sự cố về an toàn thông tin năm 2019".

Sở Thông tin và Truyền thông thông báo mời và kính đề nghị Quý cơ quan cử cán bộ tham gia đợt diễn tập nêu trên, với các nội dung cụ thể như sau:

1. Thời gian: 02 ngày, bắt đầu từ 7h00 ngày 19/12/2019 đến ngày 20/12/2019.

2. Địa điểm: Khách sạn Mỹ Trà (tầng 2), Phường Trương Quang Trọng, Thành phố Quảng Ngãi (phía Bắc cầu Trà Khúc cũ).

3. Nội dung diễn tập: *Kèm theo ở phần phụ lục.*

4. Thành viên tham dự:

- Theo Quyết định số 2459/QĐ-UBND ngày 18/12/2017 của Chủ tịch UBND tỉnh Quảng Ngãi.

- Đối với các đơn vị chưa có thành viên trong Đội ứng cứu hoặc thành viên trong đội ứng cứu của đơn vị đã chuyển công tác thì đề nghị đơn vị cử Cán bộ phụ trách CNTT tham dự.

5. Kinh phí: Ban Tổ chức lớp học chi trả các chi phí liên quan đến công tác tổ chức diễn tập; các khoản chi phí khác do đơn vị có cán bộ tham dự diễn tập chi trả theo quy định hiện hành.

Mọi chi tiết xin liên hệ: Đ.c Tín Dũng, Phòng CNTT (0944449168).

Kính đề nghị các cơ quan, đơn vị tạo điều kiện thuận lợi để các học viên tham gia tập đầy đủ và đạt kết quả tốt trong quá trình tham gia diễn tập.

Trân trọng./.

Nơi nhận:
- Như trên;
- Sở Nội vụ (để biết phối hợp);
- Vncert (để biết thực hiện);
- Sở TT&TT: GĐ, các PGĐ, các phòng ban, đơn vị;
- Lưu: VT, CNTTdungtt.

GIÁM ĐỐC

SỞ THÔNG TIN VÀ TRUYỀN THÔNG

Nguyễn Thanh Sơn

PHỤ LỤC

(Kèm theo Công văn số: / STTTT ngày 12/12/2019)

NỘI DUNG CHƯƠNG TRÌNH.

PHẦN 1. TẬP HUẤN, HUẤN LUYỆN PHỤC VỤ DIỄN TẬP.

1	Giới thiệu chức năng, nhiệm vụ của các CERT quốc tế, VNCERT/CC
2	**Tổng quan về an toàn thông tin đối với hệ thống**
2.1	Khái niêm An toàn thông tin.
2.2	Khái niệm Hệ thống thông tin.
2.3	Cách thức đảm bảo an toàn thông tin cho các hệ thống thông tin.
2.4	**An toàn thông tin đối với hệ thống mạng** Thực trạng mất an toàn, an ninh mạng Một số giải pháp đảm bảo an toàn, an ninh cho hệ thống mạng Một số khuyến nghị
3	**An toàn thông tin và một số kiểu tấn công phổ biến**
3.1	IoT và đảm bảo an toàn thông tin
3.2	Một số hình thức tấn công phổ biến
	Tấn công vào máy chủ hoặc máy trạm độc lập
	Tấn công bằng cách phá mật khẩu
	Tấn công bằng mã độc
	Tấn công quét cổng
	Tấn công từ chối dịch vụ
	Tấn công định tuyến nguồn
	Tấn công giả mạo
	Tấn công sử dụng email
	Tấn công không dây
4	***An toàn* khi sử dụng mạng Internet và Email**
5	**5. Mã độc, phần mềm độc hại**
5.1	Giới thiệu về mã độc/phần mềm độc hại
5.2	Phân loại về mã độc/phần mềm độc hại
5.3	Cách thức lây nhiễm mã độc/phần mềm độc hại
5.4	Ảnh hưởng, tác hại của mã độc/phần mềm độc hại
5.5	Các ví dụ
6.	**Xử lý sự cố virus máy tính**
6.1	Khái niệm sự cố
6.2	Quy trình xử lý sự cố
6.3	Giới thiệu vè phân tích mã độc
6.4	Môi trường và phương pháp phân tích mã độc
7	Xây dựng Lab phân tích mã độc (copy sẵn cho học viên). Hướng dẫn để có thể làm được diễn tập

PHẦN 2: KỊCH BẢN DIỄN TẬP BẢO ĐẢM AN TOÀN THÔNG TIN TRONG CƠ QUAN NHÀ NƯỚC CỦA TỈNH QUANG NGÃI NĂM 2019

<u>Chủ đề:</u> Xử lý tình huống tấn công lây nhiễm, phát tán mã độc dạng APT gây lộ lọt thông tin trên hệ thống mạng của tỉnh.

1. Kịch bản tình huống

Một Cơ quan XYZ của tỉnh Quảng Ngãi đang nghi ngờ gặp sự cố về an toàn thông tin mạng, và đề nghị Sở Thông tin và Truyền thông của Quảng Ngãi hỗ trợ xử lý và điều tra tìm nguồn gốc sự cố.

Thông tin cung cấp ban đầu cho biết, tại Cơ quan XYZ, một cán bộ Abc đang sử dụng email có địa chỉ là vanphong@quangngai.gov.vn vừa nhận email từ người có tên là Nguyễn Thanh Trà với địa chỉ nttra@actvn.edu.vn, tiêu đề thư là "CV ứng tuyển vị trí thực tập" và người này đã đọc thư và mở tập tin đính kèm. Hiện tại hệ thống mạng Cơ quan XYZ xuất hiện một số kết nối đáng ngờ.

2. Yêu cầu từ người tham gia diễn tập

Các cán bộ tham gia diễn tập phối hợp cùng với Sở Thông tin và Truyền thông Quảng Ngãi thực hiện điều tra, phân tích và tìm nguyên nhân sự cố như sau:

STT	Nội dung	Chú thích
1	1.1 Tìm tệp tin chữa mã độc trong Phishingmail.zip là email được xuất ra nghi ngờ có mã độc bên trong, trong số đó là các email có mã độc gây nên lây nhiễm. 1.2. Địa chỉ IP phát tán thư điện tử giả mạo là gì? 1.3. Xác định ASN (Autonomous System Number) và Resolve Host của địa chỉ IP phát tán	
2	2.1 Tìm Hash MD5 của tệp tin được đính kèm theo email gửi từ email giải mạo. 2.2 Tên đầy đủ bao gồm cả phần mở rộng của tệp tin khi giải nén tệp tin đính kèm theo email gửi từ email giải mạo. 2.3 Tìm Hash MD5 của tệp tin được giải nén từ tệp đính kèm theo email gửi từ email giải mạo	
3	3.1 Sau khi kích hoạt mã độc để tiến hành phân tích, mã độc đã tạo ra những tệp tin nào chạy powershell? 3.2 Tìm mã Hash MD5 của tệp tin chạy powershell? 3.3 Tên tệp tin nào là vật chứa (drop file) tạo ra mã độc kết	

	nối tới máy chủ C&C. 3.4 Hash MD5 tệp tin nào là vật chứa (drop file) tạo ra mã độc kết nối tới máy chủ điều khiển (C&C). 3.5 Mã độc có tạo ra một tệp tin tài liệu, tên tệp tin đó là gì? 3.6 Tệp tin nào là mã độc giả một trương trình trong tiến trình của window (process) có nhiệm vụ kết nối tới máy chủ C&C. 3.7 Tìm Hash của tệp tin trong tiến trình của window (process) kết nối tới máy chủ C&C.	
4	4.1 Địa chỉ IP C&C và port mã độc tới? File Pcap : pcap.zip 4.2 ASN (Autonomous System Number) và Resolve Host của địa chỉ IP phát tán	
5	5.1 Khi có kết nối tới C&C mã độc đã đặt tên cho máy bị lây nhiễm là gì? 5.2 C&C server đã thu thập tên máy, ngày kết nối, và version của window? 5.3 C&C đã thu thập được các tài khoản của diễn đàn nào? 5.4 C&C thu thập được người dùng truy cập vào website nào của tỉnh Quang ngãi? 5.5 C&C thu thập được tài khoản cũng như mật khẩu để truy cập facebook?	
6	6.1 Hacker truy cập vào thư mục nào để thu thập (download) dữ liệu? (cú pháp: C or D:\ forlder\forlder\ … 6.2 Lệnh hacker đã chạy trên máy tính bị nhiễm mã độc 6.3 Thư mục (forlder) mới được tạo trên máy nạn nhận?	
7	Báo cáo sự cố về VNCERT/CC – CATTT Cung cấp sơ đồ chi tiết về sự cố, các bạn có thể vẽ ra giấy hay là paint, visio – không thành vấn đề, miến là chính xác, chúng tôi sẽ cung cấp Flag. (Sơ đồ bao gồm tất cả các địa chỉ IP, máy tính bị lây nhiễm các tương tác, cổng kết nối)	
Bonus	Một ngọn núi và một dòng sông, hãy tìm ẩn nghĩa của nó? …..	

Danh sách mời tham dự (Văn thư biết, để Anh dungtt tham gia viết cho ok)
(Đội ứng cứu sự cố an toàn thông tin mạng tỉnh Quảng Ngãi)

TT	Họ tên	Chức vụ, Đơn vị công tác	Chức vụ trong Đội
1	Nguyễn Thanh Sơn	Giám đốc Sở Thông tin và Truyền thông	Đội trưởng (để biết, ko viết mời)
2	Nguyễn Ngọc Trân	Giám đốc Trung tâm công nghệ Thông tin và Truyền thông, Sở Thông tin và Truyền thông	Đội phó thường trực (để biết, ko viết mời)
3	Nguyễn Quốc Huy Hoàng	Trưởng phòng Công nghệ thông tin, Sở Thông tin và Truyền thông	Đội phó(để biết, ko viết mời)
4	Võ Thị Quyên	Phó Giám đốc Trung tâm công nghệ Thông tin và Truyền thông, Sở Thông tin và Truyền thông	Đội phó
5	Võ Thi Thơ	Ban quản lý KKT Dung Quất và các KCN tỉnh	Thành viên
6	Trần Long Hoanh	Báo Quảng Ngãi	Thành viên
7	Lê Văn Thịnh	Bộ Chỉ huy Bộ đội Biên phòng tỉnh Quảng Ngãi	Thành viên
8	Nguyễn Văn Tuấn	Bộ chỉ huy Quân sự tỉnh	Thành viên
9	Phạm Hồng Phi	Cảng vụ hàng hải	Thành viên
10	Trần Anh Pháp	Công an tỉnh	Thành viên
11	Trương Thanh Tịnh	Cục Hải quan tỉnh	Thành viên
12	Đinh Nguyên Bảo	Cục Thống kê tỉnh	Thành viên
13	Nguyễn Quốc Văn	Cục Thuế tỉnh	Thành viên
14	Huỳnh Quốc Bảo	Đài Phát thanh và Truyền hình tỉnh Quảng Ngãi	Thành viên
15	Hồ Tấn Sanh	Kho bạc Nhà nước tỉnh	Thành viên
16	Lê Phi Uấn	Liên Đoàn lao động tỉnh	Thành viên
17	Võ Thừa Ân	Phòng Cơ yếu-CNTT, Văn phòng Tỉnh ủy	Thành viên
18	Phạm Minh Viễn	Phòng Văn hóa và Thông tin	Thành viên

TT	Họ tên	Chức vụ, Đơn vị công tác	Chức vụ trong Đội
		huyện Ba Tơ	
19	Lê Quang Liên	Phòng Văn hóa và Thông tin huyện Đức Phổ	Thành viên
20	Nguyễn Thị Như Hiếu	Phòng Văn hóa và Thông tin huyện Mộ Đức	Thành viên (Đã chuyển công tác)
21	Phạm Hồng Thắm	Phòng Văn hóa và Thông tin huyện Sơn Tịnh	Thành viên
22	Nguyễn Việt Cường	Phòng Văn hóa và Thông tin huyện Trà Bồng	Thành viên
23	Nguyễn Duy Phú	Sở Công thương	Thành viên (thay cán bộ khác)
24	Võ Thành Phước	Sở Giáo dục và Đào tạo	Thành viên
25	Huỳnh Tấn Dũng	Sở Giao thông vận tải	Thành viên
26	Trương Quang Bảo	Sở Kế hoạch và Đầu tư	Thành viên Mời thêm Sỹ đang phụ trách
27	Trần Toàn Thắng	Sở Khoa học và Công nghệ	Thành viên. Mời thêm cán bộ đang phụ trách khác
28	Bùi Trần Quang Mẫn	Sở Lao động – Thương binh và Xã hội	Thành viên
29	Hồ Thị Thu Lệ	Sở Ngoại vụ	Thành viên
30	Trần Hồng Nhân	Sở Nội vụ	Thành viên
31	Lê Thành Trung	Sở Nông nghiệp và PTNT	Thành viên
32	Võ Đức Anh	Sở Tài chính	Thành viên
33	Lê Văn Tạo	Sở Tài nguyên và Môi Trường	Thành viên
34	Trương Tín Dũng	Sở Thông tin và Truyền thông	Thành viên
35	Nguyễn Trọng Chiến	Sở Tư pháp	Thành viên. Mời thêm thành viên

TT	Họ tên	Chức vụ, Đơn vị công tác	Chức vụ trong Đội
			khác đang phụ trách.
36	Nguyễn Phước Truyền	Sở Văn hóa, Thể thao và Du lịch	Thành viên
37	Võ Văn Hùng	Sở Xây dựng	Thành viên
38	Vương Thị Hạnh	Sở Y tế	Thành viên
39	Trần Kim Tuấn	Thanh Tra tỉnh	Thành viên
40	Lê Thanh Trang	Trung tâm Công báo và Tin học, Văn phòng UBND tỉnh	Thành viên
41	Phạm Văn Thanh	Trung tâm Công báo và Tin học, Văn phòng UBND tỉnh	Thành viên. Mời thêm Thiện Trung tâm CBTH
42	Nguyễn Công Nguyên	Trung tâm công nghệ Thông tin và Truyền thông, Sở Thông tin và Truyền thông	Thành viên
~~43~~	~~Nguyễn Tấn Linh~~	~~Trung tâm công nghệ Thông tin và Truyền thông, Sở Thông tin và Truyền thông~~	~~Thành viên~~
44	Phạm Thị Ngọc Yến	Trung tâm công nghệ Thông tin và Truyền thông, Sở Thông tin và Truyền thông	Thành viên
45	Trương Thị Diệu Thủy	Trung tâm công nghệ Thông tin và Truyền thông, Sở Thông tin và Truyền thông	Thành viên
46	Lê Tấn Sĩ	Trường Đại học Phạm Văn Đồng	Thành viên
47	Nguyễn Hồng Anh	Trường Đại học Phạm Văn Đồng	Thành viên
48	Trần Xuân Diệu	TT CNTT – Viettel Quảng Ngãi	Thành viên
49	Đồng Huân Chương	UBMT Tổ quốc Việt Nam tỉnh Quảng Ngãi	Thành viên
50	Trần Quốc Tuấn	Văn phòng HĐND&UBND huyện Bình Sơn	Thành viên. Mời thêm Anh Minh
51	Võ Ngọc Nghĩa	Văn Phòng HĐND&UBND huyện Lý Sơn	Thành viên. Mời thêm

TT	Họ tên	Chức vụ, Đơn vị công tác	Chức vụ trong Đội
			Long
52	Huỳnh Đoàn Duẩn	Văn phòng HĐND&UBND huyện Minh Long	Thành viên. Đã nghỉ việc, Mời Võ Thanh Thức thay thế
53	Võ Thế Duy	Văn phòng HĐND&UBND huyện Nghĩa Hành	Thành viên. Đã nghỉ việc, mời C.Nhuận thay thế.
54	Lê Như Hổ	Văn phòng HĐND&UBND huyện Sơn Hà	Thành viên
55	Nguyễn Văn Diệu	Văn Phòng HĐND&UBND huyện Sơn Tây	Thành viên
56	Huỳnh Văn Thuần	Văn phòng HĐND&UBND huyện Tây Trà	Thành viên
57	Võ Duy Nhật Bảo	Văn phòng HĐND&UBND huyện Tư Nghĩa	Thành viên
58	Trần Thường	Văn phòng HĐND&UBND thành phố Quảng Ngãi	Thành viên
59	Trần Quốc Tuấn	Văn phòng Hội đồng nhân dân tỉnh	Thành viên
60	Trần Văn Luân	Viện Kiểm sát nhân dân tỉnh	Thành viên
61	Hà Anh Triết	Viễn thông Quảng Ngãi	Thành viên
