UBND TỈNH QUẢNG BÌNH
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

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

Số: **358**/STTTT-CNTT

V/v hướng dẫn theo dõi, ngăn chặn xử lý mã độc WannaCry

Quảng Bình, ngày 15 tháng 5 năm 2017

Kính gửi:
- Văn phòng Tỉnh ủy, Văn phòng HĐND tỉnh;
- Các sở, ban, ngành cấp tỉnh;
- Các huyện, thành, thị ủy;
- Các UBND huyện, thị xã, thành phố;
- Các cơ quan Trung ương trên địa bàn tỉnh.

Trung tâm Ứng cứu khẩn cấp sự cố máy tính Việt Nam đã có Công văn số 144/VNCERT-ĐPƯC ngày 13/5/2017 thông báo về việc theo dõi, ngăn chặn kết nối máy chủ điều khiển mã độc WannaCry; đây là mã độc rất nguy hiểm, có thể đánh cắp thông tin và mã hóa toàn bộ máy chủ của hệ thống; tin tặc khai thác và tấn công gây hậu quả nghiêm trọng.

Vào lúc 8 giờ 00 ngày 15/5/2017, Tổ ứng cứu sự cố máy tính trên địa bàn tỉnh Quảng Bình đã kịp thời gửi cảnh báo và hướng dẫn theo dõi, ngăn chặn kết nối máy chủ điều khiển mã độc WannaCry đến 42 thành viên của Tổ (qua hệ thống thư điện tử công vụ) giúp các cơ quan, đơn vị kịp thời ứng phó, vận hành an toàn hệ thống máy tính đơn vị mình.

Để tiếp tục có biện pháp phòng tránh, ngăn chặn kịp thời, bảo vệ an toàn hệ thống thông tin của cơ quan, đơn vị và cá nhân; Sở Thông tin và Truyền thông Quảng Bình đề nghị các cơ quan, đơn vị chỉ đạo cán bộ phụ trách công nghệ thông tin thực hiện khẩn cấp các công việc sau:

1. Theo dõi, ngăn chặn kết nối đến các địa chỉ máy chủ điều khiển mã độc WannaCry (*Bao gồm 33 địa chỉ IP các máy chủ điều khiển mã độc, 10 tệp tin và 22 mã băm theo phụ lục đính kèm*).

2. Nhanh chóng chóng rà soát và cập nhật các bản vá lỗi được cảnh báo trên website chính thức của Mircosoft cho các hệ thống sử dụng hệ điều hành Windows, từ Windows Server 2000 tới Windows Server 2012, Windows XP, Windows Vista, Windows 7/8/10; cập nhật vào các hệ thống bảo vệ như: IDS/IPS, Firewall … những thông tin nhận dạng về loại mã độc WannaCry này.

3. Các cơ quan, đơn vị nếu phát hiện đã có mã độc WannaCry trên máy, cần nhanh chóng cô lập vùng/máy đã phát hiện và báo cáo gấp về Sở Thông tin và Truyền thông để phối hợp xử lý.

Trong quá trình thực hiện nếu có khó khăn, vướng mắc, gửi văn bản hoặc liên hệ trực tiếp đến Sở Thông tin và Truyền thông để cùng phối hợp xử lý. Địa chỉ liên hệ: Số 02 Hương Giang- Đồng Hới- Quảng Bình, điện thoại: 0232.3856696, hộp thư: ungcuusuco@quangbinh.gov.vn.

Nơi nhận:
- Như trên;
- Lưu: VT, CNTT.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

Nguyễn Phi Khanh

PHỤ LỤC

1. Danh sách địa chỉ các máy chủ điều khiển mã độc WannaCry

STT	Địa chỉ IP C&C	STT	Địa chỉ IP C&C
1	128.31.0.39	18	213.239.216.222
2	136.243.176.148	19	213.61.66.116
3	146.0.32.144	20	38.229.72.16
4	163.172.153.12	21	50.7.151.47
5	163.172.185.132	22	50.7.161.218
6	163.172.25.118	23	51.255.41.65
7	171.25.193.9	24	62.138.10.60
8	178.254.44.135	25	62.138.7.231
9	178.254.44.135	26	79.172.193.32
10	178.62.173.203	27	81.30.158.223
11	185.97.32.18	28	82.94.251.227
12	188.138.33.220	29	83.162.202.182
13	188.166.23.127	30	83.169.6.12
14	192.42.115.102	31	86.59.21.38
15	193.23.244.244	32	89.45.235.21
16	198.199.64.217	33	94.23.173.93
17	212.47.232.237		

2. Danh sách các tập tin chứa mã độc WannaCry.

STT	File name	STT	File Name
1	@WanaDecryptor@.exe	6	taskse.exe
2	b.wnry	7	t.wnry
3	c.wnry	8	u.wnry
4	s.wnry	9	Các file với phần mở rộng ".wnry"
5	taskdl.exe	10	Các file với phần mở rộng ".WNCRY"

3. Danh sách các mã băm

STT	SHA-256
1	ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e4
2	c365ddaa345cfcaff3d629505572a484cff5221933d68e4a52130b8bb7bad
3	09a46b3e1be080745a6d8d88d6b5bd351b1c7586ae0dc94d0c238ee36421
4	0a73291ab5607aef7db23863cf8e72f55bcb3c273bb47f00edf011515aeb5
5	428f22a9afd2797ede7c0583d34a052c32693cbb55f567a60298587b6e67
6	5c1f4f69c45cff9725d9969f9ffcf79d07bd0f624e06cfa5bcbacd2211046ed
7	62d828ee000e44f670ba322644c2351fe31af5b88a98f2b2ce27e423dcf1d
8	72af12d8139a80f317e851a60027fdf208871ed334c12637f49d819ab4b03
9	85ce324b8f78021ecfc9b811c748f19b82e61bb093ff64f2eab457f9ef19b1
10	a1d9cd6f189beff28a0a49b10f8fe4510128471f004b3e4283ddc7f7859490
11	a93ee7ea13238bd038bcbec635f39619db566145498fe6e0ea60e6e76d614
12	b43b234012b8233b3df6adb7c0a3b2b13cc2354dd6de27e092873bf58af2
13	eb47cd6a937221411bb8daf35900a9897fb234160087089a064066a65f42
14	24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1
15	2c2d8bc91564050cf073745f1b117f4ffdd6470e87166abdfcd10ecdff040a
16	7a828afd2abf153d840938090d498072b7e507c7021e4cdd8c6baf727cafc
17	a897345b68191fd36f8cefb52e6a77acb2367432abb648b9ae0a9d708406d
18	fb0b6044347e972e21b6c376e37e1115dab494a2c6b9fb28b92b1e45b45d
19	9588f2ef06b7e1c8509f32d8eddfa18041a9cc15b1c90d6da484a39f8dcdf9
20	b43b234012b8233b3df6adb7c0a3b2b13cc2354dd6de27e092873bf58af2
21	4186675cb6706f9d51167fb0f14cd3f8fcfb0065093f62b10a15f7d9a6c8d9
22	09a46b3e1be080745a6d8d88d6b5bd351b1c7586ae0dc94d0c238ee36421