BỘ Y TẾ **CỤC CÔNG NGHỆ THÔNG TIN**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập – Tự do – Hạnh phúc**
Số: 173 /CNTT-CSHT V/v theo dõi, phòng chống mã độc WannaCry	*Hà Nội, ngày 17 tháng 5 năm 2017*

Kính gửi:

- Các Vụ, Cục, Tổng cục, Văn phòng Bộ, Thanh tra Bộ;
- Các đơn vị trực thuộc Bộ Y tế;
- Sở Y tế các tỉnh, thành phố trực thuộc Trung ương.

Nhằm phòng ngừa, ngăn chặn việc tấn công của mã độc Ransomware WannaCry (hoặc được biết với các tên khác như: WannaCrypt, WanaCryptOr 2.0, ...) vào Việt Nam, ngày 13/5/2017 Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam VNCERT đã có công văn số 144/VNCERT-ĐPƯC 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 dữ liệu trong máy chủ hệ thống cũng như máy tính cá nhân, gây nên nhiều hậu quả nghiêm trọng khác. Vì vậy, Cục Công nghệ thông tin đề nghị các đơn vị thực hiện khẩn cấp các việc sau đây:

1. Đối với cán bộ, công chức, viên chức, người lao động:

- Không nhấp vào các đường liên kết, tập tin đính kèm và biểu tượng quảng cáo không rõ nguồn gốc.

- Khi xảy ra sự cố, nhanh chóng ngừng sử dụng máy tính, ngắt kết nối mạng và báo ngay với tổ chức và cá nhân chuyên trách về công nghệ thông tin.

2. Đối với tổ chức chuyên trách công nghệ thông tin:

- Kiểm tra, hướng dẫn, thực hiện cập nhật bản vá các lỗ hổng bảo mật trên hệ điều hành, ứng dụng đối với các máy tính cá nhân, máy chủ của đơn vị.

- Thực hiện sao lưu ngay các dữ liệu quan trọng của đơn vị và để cách ly an toàn.

- Theo dõi, ngăn chặn kết nối đến các máy chủ điều khiển mã độc WannaCry và cập nhật vào các hệ thống bảo vệ như IDS/IPS, Firewall… các thông tin nhận dạng tại phụ lục đính kèm.

- Sử dụng các phần mềm có khả năng phát hiện và tiêu diệt mã độc để rà quét toàn bộ hệ thống.

Lãnh đạo các đơn vị chủ động giám sát, chỉ đạo kịp thời công tác tổ chức phòng, chống mã độc, đảm bảo an toàn dữ liệu và hoạt động chung của đơn vị.

Xin trân trọng cảm ơn!

Nơi nhận:
- Như trên;
- Thứ trưởng Lê Quang Cường (để b/c);
- Cục trưởng (để b/c);
- Lưu: VT, CSHT.

KT. CỤC TRƯỞNG
PHÓ CỤC TRƯỞNG

CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM
CỤC CÔNG NGHỆ THÔNG TIN

Lương Chí Thành

BỘ Y TẾ
CỤC CÔNG NGHỆ THÔNG TIN

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

PHỤ LỤC
THÔNG TIN VỀ MÃ ĐỘC WANNACRY

(kèm theo công văn số 173 /CNTT-CSHT ngày 17 tháng 5 năm 2017 của Cục Công nghệ thông tin)

A. Danh sách các máy chủ điều khiển mã độc (C&C Server)

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		

B. Danh sách tên tập tin

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"

C. Danh sách mã băm (Hash SHA-256)

STT	SHA-256
1	ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa
2	c365ddaa345cfcaff3d629505572a484cff5221933d68e4a52130b8bb7badaf9
3	09a46b3e1be080745a6d8d88d6b5bd351b1c7586ae0dc94d0c238ee36421cafa
4	0a73291ab5607aef7db23863cf8e72f55bcb3c273bb47f00edf011515aeb5894
5	428f22a9afd2797ede7c0583d34a052c32693cbb55f567a60298587b6e675c6f
6	5c1f4f69c45cff9725d9969f9ffcf79d07bd0f624e06cfa5bcbacd2211046ed6
7	62d828ee000e44f670ba322644c2351fe31af5b88a98f2b2ce27e423dcf1d1b1
8	72af12d8139a80f317e851a60027fdf208871ed334c12637f49d819ab4b033dd
9	85ce324b8f78021ecfc9b811c748f19b82e61bb093ff64f2eab457f9ef19b186
10	a1d9cd6f189beff28a0a49b10f8fe4510128471f004b3e4283ddc7f78594906b
11	a93ee7ea13238bd038bcbec635f39619db566145498fe6e0ea60e6e76d614bd3
12	b43b234012b8233b3df6adb7c0a3b2b13cc2354dd6de27e092873bf58af2693c
13	eb47cd6a937221411bb8daf35900a9897fb234160087089a064066a65f42bcd4
14	24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c
15	2c2d8bc91564050cf073745f1b117f4ffdd6470e87166abdfcd10ecdff040a2e
16	7a828afd2abf153d840938090d498072b7e507c7021e4cdd8c6baf727cafc545
17	a897345b68191fd36f8cefb52e6a77acb2367432abb648b9ae0a9d708406de5b
18	fb0b6044347e972e21b6c376e37e1115dab494a2c6b9fb28b92b1e45b45d0ebc
19	9588f2ef06b7e1c8509f32d8eddfa18041a9cc15b1c90d6da484a39f8dcdf967
20	b43b234012b8233b3df6adb7c0a3b2b13cc2354dd6de27e092873bf58af2693c
21	4186675cb6706f9d51167fb0f14cd3f8fcfb0065093f62b10a15f7d9a6c8d982
22	09a46b3e1be080745a6d8d88d6b5bd351b1c7586ae0dc94d0c238ee36421cafa