BỘ NÔNG NGHIỆP
VÀ PHÁT TRIỂN NÔNG THÔN
TỔNG CỤC LÂM NGHIỆP

Số. 687 /TCLN-VP
V/v cảnh báo mã độc WannaCry

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

Hà Nội, ngày 15 tháng 5 năm 2017

Kính gửi: - Các đơn vị thuộc Tổng cục Lâm nghiệp;
- Dự án FORMIS II.

Vừa qua, mã độc tống tiền (ransomware) có tên WannaCry đã tấn công và lan rộng khắp thế giới khiến hơn 200.000 máy tính tại hơn 150 quốc gia, trong đó có Việt Nam, đã bị khóa dữ liệu và đòi tiền chuộc. Đây là mã độc rất nguy hiểm, có thể đánh cắp thông tin và mã hóa toàn bộ hệ thống máy tính của tổ chức bị hại. Khi bị nhiễm mã độc WannaCry, người dùng sẽ khó phát hiện cho đến khi nó tự gửi thông báo cho biết máy tính đã bị khóa, mọi tập tin đã bị mã hóa và không thể sử dụng.

Để hạn chế khả năng bị tấn công đến mức tối thiểu, Tổng cục xin thông báo để các đơn vị biết và có biện pháp phòng ngừa, cụ thể như sau:

1. Đối với các cá nhân và đơn vị thuộc Tổng cục:

- Sao lưu ngay dữ liệu quan trọng bằng thiết bị lưu trữ ngoài.
- Cập nhật phiên bản mới nhất của chương trình diệt virus.
- Cập nhật các bản vá lỗi Windows mới nhất thông qua Windows Update (Control Panel -> Windows Update -> Check for updates).
- Không mở e-mail lạ cũng như không tải các tập tin đính kèm e-mail đó.
- Hạn chế truy cập vào các trang web nước ngoài, các trang web lạ.
- Không bấm vào các link có đuôi .hta hoặc link không rõ nguồn gốc, có cấu trúc không rõ ràng.

2. Đối với Dự án FORMIS II:

- Kiểm tra ngay hệ thống bảo mật, Firewall của các máy chủ, nhanh chóng rà soát và cập nhật các bản vá lỗi từ Microsoft.
- Tạm thời khóa các dịch vụ sử dụng cổng 445/137/138/139 (nếu có).
- Ngăn chặn kết nối đến các máy chủ điều khiển mã độc WannaCry và cập nhật vào hệ thống bảo vệ.
- Tạo bản snapshot đối với các máy chủ ảo hóa để phòng việc bị tấn công.
- Tăng cường theo dõi, giám sát và bảo vệ hệ thống trong thời điểm này.

(Kèm theo Văn bản 144/VNCERT-ĐPƯC ngày 13/5/2017 của TT ƯCKH máy tính VN)

Tổng cục thông báo để các đơn vị biết, thực hiện./.

Nơi nhận:
- Như trên;
- Thứ trưởng TT Hà Công Tuấn (b/c);
- Lãnh đạo Tổng cục (b/c);
- Lưu: VT, VP (DLTH).(30)

TL. TỔNG CỤC TRƯỞNG
CHÁNH VĂN PHÒNG

Nguyễn Bình Minh

BỘ THÔNG TIN VÀ TRUYỀN THÔNG
TRUNG TÂM ỨNG CỨU KHẨN CẤP MÁY TÍNH VIỆT NAM

Số: 144/VNCERT-ĐPƯC
V/v theo dõi, ngăn chặn kết nối máy chủ điều khiển mã độc WannaCry

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

Hà Nội, ngày 13 tháng 5 năm 2017

Kính gửi:

- Các đơn vị chuyên trách về CNTT, ATTT Văn phòng Trung ương Đảng, Văn phòng Chủ tịch nước, Văn phòng Quốc hội, Văn phòng Chính phủ;
- Các đơn vị chuyên trách về CNTT, ATTT các Bộ, Ngành;
- Các đơn vị thuộc Bộ Thông tin và Truyền thông;
- Các Sở thông tin và Truyền thông;
- Thành viên mạng lưới ứng cứu sự cố Internet Việt Nam;
- Các Tổng công ty, Tập đoàn kinh tế; Tổ chức tài chính và ngân hàng; các Doanh nghiệp hạ tầng Internet, Viễn thông, Điện lực, Hàng không, Giao thông vận tải.

Thực hiện Thông tư 27/2011/TT-BTTTT về điều phối các hoạt động ứng cứu sự cố mạng Internet Việt Nam, Trung tâm VNCERT yêu cầu Lãnh đạo đơn vị chỉ đạo các đơn vị thuộc phạm vi quản lý thực hiện khẩn cấp các việc sau để phòng ngừa, ngăn chặn việc tấn công của mã độc Ransomware WannaCry (hoặc được biết với các tên khác như: WannaCrypt, WanaCrypt0r 2.0, ...) vào Việt Nam:

1. Theo dõi, ngăn chặn kết nối đến các máy chủ 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;

2. Nếu phát hiện cần nhanh chóng cô lập vùng/máy đã phát hiện;

3.Kiểm tra và thực hiện gấp các bước đã được hướng dẫn trước đây tại văn bản số 80/VNCERT-ĐPƯC, ngày 09/3/2016 và văn bản 123/VNCERT-ĐPƯC, ngày 24/4/2017, tải tại địa chỉ:

http://www.vncert.gov.vn/baiviet.php?id=24
http://vncert.gov.vn/baiviet.php?id=52 ;

để phòng tránh các cuộc tấn công qui mô lớn và nguy hiểm khác;

4. Sau khi thực hiện, yêu cầu các đơn vị báo cáo tình hình về Đầu mối điều phối ứng cứu sự cố quốc gia (Trung tâm VNCERT) theo địa chỉ email: ir@vncert.gov.vn;

5. Trên đây là mã độc rất nguy hiểm, có thể đánh cắp thông tin và mã hóa toàn bộ máy chủ hệ thống đồng thời với các lỗ hổng đã công bố, Tin tặc khai thác và tấn công sẽ gây lên nhiều hậu quả nghiêm trọng khác, Trung tâm VNCERT yêu cầu Lãnh đạo các đơn vị nghiêm túc thực hiện lệnh điều phối.

Trân trọng./.

KT.GIÁM ĐỐC
PHÓ GIÁM ĐỐC

BỘ THÔNG TIN VÀ TRUYỀN THÔNG
TRUNG TÂM ỨNG CỨU KHẨN CẤP MÁY TÍNH VIỆT NAM

Nguyễn Khắc Lịch

Nơi nhận:
- Như trên;
- Bộ trưởng Trương Minh Tuấn (để b/c);
- Thứ trưởng Nguyễn Thành Hưng (để b/c);
- Giám đốc (để b/c);
- Các phòng, chi nhánh: KTHT, NCPT, TVĐT, CNHCM, CNĐN;
- Lưu VT, ĐPƯC.

BỘ THÔNG TIN VÀ TRUYỀN THÔNG
TRUNG TÂM ỨNG CỨU KHẨN CẤP MÁY TÍNH VIỆT NAM

TRUNG TÂM ỨNG CỨU KHẨN CẤP MÁY TÍNH VIỆT NAM

PHỤ LỤC
THÔNG TIN VỀ MÃ ĐỘC WANNACRY

(kèm theo công văn số 144/VNCERT-ĐPƯC ngày 13/5/2017)

I. 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		

II. 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"

III. Danh sách mã băm (Hash SHA-256)

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