UBND TỈNH ĐẮK LẮK
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

Số: 334/STTTT-CNTT
V/v phòng ngừa, ngăn chặn mã độc tống tiền Ransomware WannaCry

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

Đắk Lắk, ngày 15 tháng 5 năm 2017

Kính gửi:
- Văn phòng Tỉnh ủy;
- Văn phòng HĐND tỉnh;
- Văn phòng UBND tỉnh;
- Các sở, ban, ngành, đoàn thể của tỉnh;
- UBND các Huyện, Thị xã, Thành phố;

HỎA TỐC

Trong những ngày qua, trên môi trường mạng Internet đã xuất hiện mã độc Ransomware WannaCry (hoặc được biết với các tên khác như WannaCrypt, Wanna Crypt0r, WanaCrypt0r 2.0, ...) lây lan nhanh chóng trên toàn thế giới, chỉ trong vài giờ đã lây nhiễm hơn 100 ngàn máy tính tại 74 quốc gia trên thế giới. Theo ghi nhận của các tổ chức an toàn thông tin của Việt Nam, ngày 13/5/2017, mã độc Ransomware WannaCry cũng đã lây nhiễm vào một số máy tính của Việt Nam và có nguy cơ bùng phát.

Đây là mã độc rất nguy hiểm, có thể đánh cắp thông tin và mã hóa toàn bộ máy chủ hệ thống, phương thức lây nhiễm của Ransomware WannaCry tấn công vào máy tính thông thường là thông qua các tập tin đính kèm thư điện tử (email) hoặc đường dẫn (link) nhúng mã độc giống như cách tấn công của các loại mã độc tống tiền khác. Tuy nhiên, dòng mã độc này được bổ sung khả năng lây nhiễm trên các máy tính kết nối mạng.

Cụ thể, khi có một máy tính trong hệ thống mạng nội bộ (LAN) bị nhiễm, Ransomware WannaCry sẽ tiến hành quét toàn bộ các máy tính trong cùng mạng nội bộ để tìm kiếm các máy tính, thiết bị khác có lỗ hổng EternalBlue của dịch vụ SMB (trên hệ điều hành Windows). Từ đó, mã độc có thể lây lan vào các máy có lỗ hổng mà không cần người dùng phải thao tác trực tiếp với tập tin đính kèm hoặc đường dẫn có mã độc.

Khi máy tính bị nhiễm Ransomware WannaCry, tất cả các dữ liệu trong máy tính đó đều bị mã hóa các nạn nhân được yêu cầu nộp số tiền chuộc là 300 đồng tiền ảo Bitcoin để mở khóa. Nạn nhân chỉ có 03 ngày để nộp tiền chuộc, sau 03 ngày giá tiền sẽ tăng gấp đôi, còn sau 07 ngày nếu vẫn không trả tiền, các dữ liệu đó sẽ vĩnh viễn không thể phục hồi được.

Để tăng cường công tác đảm bảo an toàn thông tin cho hệ thống thông tin trong các cơ quan, đơn vị nhà nước, đặc biệt là để phòng ngừa, ngăn chặn mã độc tống tiền Ransomware WannaCry, Sở Thông tin và Truyền thông đề nghị các cơ quan, đơn vị thực hiện một số nội dung sau:

1. Tổ chức kiểm tra, rà soát, theo dõi, ngăn chặn kết nối đến các máy chủ máy chủ điều khiển mã độc Ransomware WannaCry và cập nhật vào các hệ thống bảo vệ

như: IDS/IPS, Firewall, ... các thông tin nhận dạng theo khuyến cáo của VNCERT *(có phô tô kèm theo)*.

2. Thực hiện ngay các biện pháp khắc phục các lỗ hổng bảo mật tồn tại trên hệ thống công nghệ thông tin, cập nhật các bản vá mới nhất của hệ điều hành, phần mềm chống virus, phần mềm văn phòng MS Office, ...

3. Đối với các hệ thống thư điện tử: Nghiêm túc thực hiện biện pháp bảo đảm an toàn thông tin theo các hướng dẫn của Bộ Thông tin và Truyền thông tại Văn bản số 430/BTTTT-CATTT ngày 09/02/2015 về việc hướng dẫn bảo đảm an toàn thông tin cho hệ thống thư điện tử của cơ quan, tổ chức nhà nước. Không thực hiện mở các địa chỉ thư điện tử có đường dẫn hoặc tập tin (file) đính kèm không tin tưởng.

4. Nếu phát hiện máy tính bị nhiễm mã độc Ransomware WannaCry cần nhanh chóng cô lập vùng/máy đã phát hiện.

5. Tăng cường theo dõi, giám sát về mặt nội dung, kỹ thuật hoạt động của các hệ thống thông tin nhằm phát hiện kịp thời các sự cố và các dấu hiệu tấn công. Trong trường hợp phát hiện các dấu hiệu tấn công cần sớm có biện pháp khắc phục. Trong trường hợp sự cố nghiêm trọng cần thông báo ngay cho Sở Thông tin và Truyền thông để kịp thời có biện pháp phối hợp xử lý.

6. 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 của VNCERT *(phô tô kèm theo)* để phòng tránh các cuộc tấn công quy mô lớn và nguy hiểm khác.

Nhận được Công văn này, đề nghị Thủ trưởng các cơ quan, đơn vị của tỉnh, Chủ tịch UBND các huyện, thị xã, thành phố triển khai thực hiện, quán triệt nội dung văn bản tới toàn thể cán bộ, công chức, viên chức trực thuộc đơn vị quản lý./.

Nơi nhận:
- Như trên;
- Cục ATTT – Bộ TT&TT (để b/c);
- UBND tỉnh (để b/c);
- VNCERT;
- Công an tỉnh (để phối hợp);
- Lãnh đạo Sở;
- TT CNTT&TT, TT Cổng TTĐT;
- Lưu VT, CNTT.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
TỈNH ĐẮK LẮK

Ra Lan Trương Thanh Hà

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

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

Số: 123 /VNCERT – ĐPƯC
V/v các phương thức tấn công khai thác hệ thống mới của nhóm tin tặc Shadow Brokers.

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

Hà Nội, ngày 24 tháng 4 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 các Bộ, Ngành;
- Các đơn vị thuộc Bộ Thông tin và Truyền thông;
- Các Sở Thông tin và Truyền thông;
- Các Tập đoàn kinh tế; Tổng công ty nhà nước; Tổ chức tài chính và ngân hàng; Các doanh nghiệp hạ tầng Internet, Viễn thông, Điện lực, Hàng không, Giao thông vận tải.

Ngày 14 tháng 4 năm 2017, nhóm tin tặc có tên gọi Shadow Brokers tuyên bố đã đánh cắp được một bộ công cụ gián diệp tấn công hệ thống nhằm khai thác dữ liệu của Cơ quan An ninh mạng quốc gia Hoa Kỳ (NSA). Do không đạt được thỏa thuận về tài chính để đánh đổi bộ công cụ, nhóm tin tặc Shadow Brokers đã tung lên mạng thông qua website chuyên về mã nguồn mở Github. Bộ công cụ bao gồm các chương trình nhị phân đã được biên dịch để khai thác bất kỳ hệ thống nào sử dụng các phiên bản của hệ điều hành Windows (trừ Windows 10 và Windows Server 2016) thông qua các lỗ hổng chưa được khai thác. Mục tiêu của các công cụ tấn công này nhằm vào các tổ chức tiền tệ, ngân hàng lớn, phần đông có trụ sở tại khu vực Trung Đông như UAE, Kuwait, Qatar, Palestine và Yemen. Theo báo cáo đánh giá của các chuyên gia an toàn thông tin mạng cho thấy điều này có gây ra nguy cơ mất an toàn thông tin trên diện rộng đa quốc gia, trong đó có Việt Nam.

Thực hiện thông tư số 27/2011/TT-BTTTT ngày 04/10/2011 của Bộ Thông tin và Truyền thông quy định về điều phối các hoạt động ứng cứu sự cố

mạng Internet Việt Nam, nhằm ngăn chặn sự lây lan và giảm thiểu rủi ro cho các đơn vị nắm giữ hệ thống thông tin quan trọng, đơn vị và doanh nghiệp sử dụng giao dịch thanh toán trực tuyến và người dùng Internet, Trung tâm VNCERT yêu cầu các cơ quan, doanh nghiệp cần chú ý và tăng cường công tác bảo đảm an toàn thông tin mạng để phòng ngừa sự cố có thể xảy ra.

Các phương thức tấn công khai thác dữ liệu hệ thống được đưa ra như sau:

Một trong các công cụ Hacking được công bố gọi là Eternalromance, chứa một giao diện dễ sử dụng và khai thác hệ thống Window thông qua các cổng TCP 445 và 139. Các lỗ hổng của hệ điều hành Window được công bố gồm: EternalBlue (MS17-010), EmeraldThread (MS10-06), EternalChampion (CVE-2017-0146 và CVE-2017-0147), ErraticGopher (lỗ hổng trên Windows Vista - không được hỗ trợ), EsikmoRoll (MS14-068), EternalRomance (MS17-010), EducatedScholar (MS09-050), EternalSynergy (MS17-010), Eclipsed Wing (MS08-067).

Bên cạnh đó, nhóm tin tặc Shardow Brokers còn khai thác lỗ hổng zero-day (CVE-2016-6366) ExtraBacon qua giao thức SNMP - giao thức tầng ứng dụng trong phần mềm Cisco ASA cho phép tin tặc không cần xác thực từ xa để khởi động lại hệ thống hoặc thực thi mã tùy ý, từ đó chiếm quyền kiểm soát thiết bị. Một hành vi tấn công hệ thống của Cisco cũng được khai thác thông qua tệp tin giải mã lưu lượng mạng riêng ảo (VPN) Cisco PIX và cấy mã độc vào bo mạch chủ firmware nhằm che dấu hành vi và xóa dấu vết.

Để phòng tránh các rủi ro mất an toàn thông tin mạng liên quan đến các công cụ tấn công của nhóm tin tặc Shardow Broker đưa ra, Trung tâm VNCERT khuyến cáo các đơn vị, doanh nghiệp sử dụng các biện pháp sau:

- Đối với hệ thống sử dụng hệ điều hành Windows (từ Windows Server 2000 tới Windows Server 2012, Windows XP, Windows Vista, Windows 7, Windows 8,...) nhanh chóng rà soát và cập nhật các bản vá lỗi được cảnh báo trên tại website chính thức của Mircosoft;

- Đối với hệ thống sử dụng các thiết bị của Cisco, cập nhật các bản vá lỗi liên quan đến lỗ hổng zero - day (CVE-2016-6366). Để bảo vệ dữ liệu an toàn, máy tính nên được bảo vệ đằng sau Router hoặc Firewalls. Trang bị các hệ thống phòng chống tấn công mạng như IPS/IDS, Firewalls...;

- Cập nhật phiên bản mới nhất của các chương trình diệt Virus để phát hiện và xử lý các mã thực thi do tin tặc tấn công vào hệ thống;

- Thực hiện sao lưu dữ liệu định kỳ: Sử dụng các ổ đĩa lưu trữ ngoài như ổ cứng cắm ngoài, ổ đĩa USB để lưu trữ các dữ liệu quan trọng trong máy tính. Sau khi sao lưu xong đưa ra cất giữ riêng và không kết nối vào internet.

Để giúp các cơ quan chức năng theo dõi, phân tích và kịp thời phản ứng nhanh với các phương thức tấn công mới, ngay khi phát hiện sự cố và không có khả năng xử lý thông báo ngay về:

Đầu mối Điều phối ứng cứu sự cố Quốc gia:

Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam - VNCERT

- Địa chỉ: Tầng 5, Tòa nhà 115 Trần Duy Hưng, Cầu Giấy, Hà Nội;

- Điện thoại: 04 3640 4423 số máy lẻ 112;

- Đường dây nóng: 0934 424 009;

- Hòm thư điện tử tiếp nhận báo cáo sự cố: ir@vncert.gov.vn.

Trân trọng./.

Nơi nhận:
- Như trên;
- Bộ trưởng (để b/c);
- Thứ trưởng Nguyễn Thành Hưng (để b/c);
- Cục ATTT, Cục BĐTW, VNNIC, NEAC;
- Giám đốc (để b/c);
- Các phòng, CN;
- Lưu VT, ĐPUC.

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

BỘ THÔNG TIN VÀ TRUYỀN THÔNG
TRUNG TÂM ỨNG CỨU KHẨN CẤP
MÁY TÍNH VIỆT NAM
Số: 80 /VNCERT-ĐPUC

Cảnh báo hình thức lây nhiễm mới của mã độc mã hoá tài liệu (Ransomware)

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

Hà Nội, ngày 09 tháng 03 năm 2016

Kính gửi:

- Các đơn vị chuyên trách về CNTT các Bộ, Ngành;
- Các Sở Thông tin và Truyền thông;
- Các nhà cung cấp dịch vụ Internet (ISP);
- Các đơn vị thuộc Bộ Thông tin và Truyền thông

Trong tuần đầu tháng 03/2016, Trung tâm VNCERT ghi nhận cách thức tấn công mới của tin tặc nhằm vào các cơ quan tổ chức có sử dụng các hòm thư điện tử nội bộ. Với cách tấn công mới này, tin tặc sẽ giả mạo một địa chỉ điện tử có đuôi là @tencongty.com.vn để gửi thư điện tử có kèm mã độc đến các người dùng trong công ty đó. Để qua mặt các hệ thống dò quét mã độc, các mã độc thường được nén lại dưới định dạng .zip hoặc .zar. Qua phân tích của chuyên gia VNCERT với một sự cố cho thấy, tệp tin chứa mã độc .zip chứa bên trong các tệp tin thực thi như .js (đây là một tệp tin Javascript) hoặc tệp tin văn bản như .doc, .xls..., khi người dùng mở tập tin này mã độc sẽ được kích hoạt và tự động tải tập tin mã độc mã hóa tài liệu và tự thực thi trên máy. Với trường hợp mã độc mã hóa tài liệu thì mã độc sẽ tiến hành mã hoá nội dung toàn bộ các dữ liệu trên máy nạn nhân với thuật toán mã hóa mạnh để không thể giải mã được với mục đích bắt các dữ liệu trên máy để tống tiền nạn nhân. Với việc giả mạo chính các địa chỉ thư điện tử của đơn vị sẽ làm cho người dùng khó phát hiện các thư giả mạo dẫn đến số lượng các máy tính bị lây nhiễm mã độc mã hóa dữ liệu có thể tăng cao.

Thực hiện Thông tư số 27/2011/TT-BTTTT ngày 04/10/2011 của Bộ Thông tin và Truyền thông quy định về điều phối các hoạt động ứng cứu sự cố mạng Internet Việt Nam, nhằm ngăn chặn sự lây lan và giảm thiểu thiệt hại cho người dùng Internet, Trung tâm VNCERT yêu cầu các cơ quan, tổ chức cần chú ý và tăng cường công tác tuyên truyền rộng rãi đến các nhân viên, người dùng máy tính để phòng ngừa sự cố có thể xảy ra.

Các phương pháp lây lan chủ yếu của mã độc mã hoá tài liệu là:

1. Gửi tập tin đính kèm thư điện tử, khi người dùng mở tập tin thì mã độc sẽ tự động lây nhiễm vào máy tính người dùng;

2. Gửi thư điện tử hoặc tin nhắn điện tử có chứa đường dẫn đến mã độc và yêu cầu người dùng tải về và cài đặt;

Ngoài ra máy tính còn có thể bị lây nhiễm thông qua đường khác như qua các thiết bị lưu trữ, qua quá trình cài đặt phần mềm không rõ nguồn gốc, sao chép dữ liệu từ máy nhiễm,...

Dấu hiệu nhận biết của loại mã độc sau khi máy tính bị nhiễm là các tài liệu, văn bản sẽ bị thay đổi nội dung và đổi tên phần mở rộng, phổ biến là các tập tin có định dạng: .doc, .docx, .pdf, .xls, .xlsx, .jpg, .txt, .ppt, .pptx,...một số loại còn khoá máy tính không cho sử dụng và đòi tiền chuộc.

Để phòng ngừa các loại mã độc Ransomware trong tình hình hiện nay, Trung tâm VNCERT khuyến cáo các đơn vị xử lý một số biện pháp sau:

1. Phòng ngừa để hạn chế tối đa khả năng bị nhiễm mã độc:

- Phân quyền hợp lý cho các loại tài khoản người dùng, bảo vệ các tập tin không cho phép xoá, sửa nội dung các tập tin quan trọng.

- Cài đặt và thường xuyên cập nhật cho hệ điều hành, phần mềm chống mã độc như Kaspersky, Symantec, Avast, AVG, MSE, Bkav, CMC,...

- Chú ý cảnh giác với các tập tin đính kèm, các đường liên kết ẩn được gửi đến thư điện tử người dùng, kể cả người gửi từ trong nội bộ.

- Thực hiện các biện pháp kỹ thuật nhằm kiểm tra xác thực người dùng trên máy chủ gửi email của đơn vị, tránh bị giả mạo người gửi từ nội bộ.

- Tắt các chế độ tự động mở, chạy tập tin đính kèm theo thư điện tử.

2. Thực hiện sao lưu dữ liệu định kỳ:

- Sử dụng các ổ đĩa lưu trữ như Ổ cứng cắm ngoài, Ổ đĩa USB để lưu trữ các dữ liệu quan trọng trong máy tính. Sau khi sao lưu xong đưa ra cất giữ riêng.

- Sử dụng các công cụ, giải pháp chuyên dụng để sao lưu dữ liệu như: các máy chủ quản lý tập tin, máy chủ sao lưu từ xa, các công cụ lưu trữ đám mây cho phép khôi phục lịch sử thay đổi của tập tin.

3. Xử lý khi phát hiện lây nhiễm mã độc:

Khi mã độc lây nhiễm vào máy tính, mã độc sẽ tiến hành quét và mã hoá các tập tin trong một khoảng thời gian. Do đó, việc phản ứng nhanh khi phát hiện ra sự cố có thể giúp giảm thiểu thiệt hại cho dữ liệu trên máy tính và tăng khả năng khôi phục dữ liệu bị mã hoá. Cụ thể cần thực hiện các thao tác sau:

- Nhanh chóng tắt máy tính bằng các ngắt nguồn điện.

- Không được khởi động lại máy tính theo cách thông thường mà phải khởi động từ hệ điều hành sạch khác (khuyến nghị hệ điều hành Linux) như từ ổ đĩa CD, USB,...sau đó thực hiện kiểm tra các tập tin dữ liệu và sao lưu các dữ liệu chưa bị mã hoá.

- Các tập tin đã bị mã hoá tương đối khó để giải mã, tuy nhiên trong một số trường hợp có thể sử dụng các phần mềm khôi phục dữ liệu như FTK, EaseUs, R-STUDIO,...để khôi phục các tập tin nguyên bản đã bị xoá.

- Cài đặt lại toàn bộ hệ thống, cài đặt phần mềm diệt virus đồng thời thiết lập chế độ cập nhật phiên bản tự động.

Để giúp các cơ quan chức năng theo dõi, phân tích và phản ứng nhanh chóng với các loại mã độc mới, ngay khi phát hiện xảy ra sự cố về mã độc Ransomware cần nhanh chóng thông báo về:

Đầu mối điều phối ứng cứu quốc gia:

Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam (VNCERT)

- Địa chỉ: 18 Nguyễn Du – Hai Bà Trưng – Hà Nội
- Điện thoại: 0436404423
- Điện thoại di động: 0934424009
- Hòm thư điện tử tiếp nhận sự cố: ir@vncert.gov.vn

Trân trọng cảm ơn./.

Nơi nhận:
- Như trên;
- Bộ Trưởng Nguyễn Bắc Son (để b/c);
- Thứ Trưởng Nguyễn Thành Hưng (để b/c);
- Cục An toàn thông tin;
- Giám đốc (để b/c);
- Chi nhánh Hồ Chí Minh;
- Chi nhánh Đà Nẵng;
- Lưu: VT, ĐPUC (01), KTHT (01).

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

TRUNG TÂM ỨNG CỨU KHẨN CẤP MÁY TÍNH VIỆT NAM

Nguyễn Khắc Lịch