UBND TỈNH THÁI BÌNH
SỞ Y TẾ

Số: 746 /SYT-KHTC

V/v giám sát, ngăn chặn khẩn cấp hệ thống máy chủ điều khiển mã độc tấn công có chủ đích ATP

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

Thái Bình, ngày 27 tháng 9 năm 2017

Kính gửi: Các đơn vị trực thuộc Sở Y tế.

Thực hiện Công văn số 420/CNTT-CSHT ngày 22/9/2017 của Cục Công nghệ thông tin - Bộ Y tế về việc giám sát, ngăn chặn khẩn cấp hệ thống máy chủ điều khiển mã độc tấn công có chủ đích ATP, loại mã độc này rất tinh vi, chúng có khả năng phát hiện các môi trường phân tích mã độc nhằm tránh phát hiện, đánh cắp dữ liệu, xâm nhập trái phép, phá hủy hệ thống thông tin thông qua các máy chủ điều khiển mã độc (C&C Server) đặt bên ngoài lãnh thổ Việt Nam. Đây là loại mã độc nguy hiểm, tin tặc có thể tấn công leo thang đặc quyền gây ra nhiều hậu quả nghiêm trọng. Để đảm bảo an toàn thông tin cho các hệ thống thông tin trong ngành Y tế, Sở Y tế yêu cầu các đơn vị thực hiện một số nội dung sau:

1. Giám sát nghiêm ngặt, ngăn chặn kết nối đến các máy chủ điều khiển mã độc APT theo danh sách trong phụ lục gửi kèm.

2. Nếu phát hiện mã độc cần nhanh chóng cô lập vùng/ máy và tieenshanhf điều tra, xử lý (cài đặt lại hệ điều hành không gỡ bỏ được triệt để).

3. Cập nhật các bản vá cho hệ điều hành và phần mềm. Đặc biệt cập nhật các lỗ hổng có CVE: CVE-2012-0158, CVE-2017-0199, MS17-010.

4. Sau khi thực hiện, đề nghị các đơn vị báo cáo tình hình lây nhiễm và kết quả xử lý (nếu có) về Sở Y tế để phối hợp xử lý./.

Nơi nhận:
- Như trên;
- GĐ, các PGĐ Sở;
- Lưu: VP, KHTC.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM
SỞ Y TẾ
TỈNH THÁI BÌNH

Trần Quang Hải

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 DOMAIN VÀ IP C&C SERVER LIÊN QUAN ĐẾN MÃ ĐỘC APT

(kèm theo công văn số 420/CNTT-CSHT ngày 22/09/2017)

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

STT	Địa chỉ IP C&C	STT	Địa chỉ IP C&C
1	209.58.179.202	10	193.169.245.78
2	209.58.176.46	11	104.237.218.72
3	188.42.254.112	12	193.169.245.137
4	66.154.125.145	13	23.227.196.210
5	176.223.165.165	14	23.227.196.214
6	60.251.29.40	15	185.157.79.3
7	103.53.197.202	16	104.237.218.70
8	58.158.177.102	17	62.210.115.97
9	216.107.152.217		

II. Danh sách tên miền máy chủ độc hại (C&C Server)

STT	Tên miền	STT	Tên miền
1	hanoi.danang.dulichovietnam.net	38	blog.docksugs.org
2	dalat.dulichovietnam.net	39	high.expbas.net
3	hanoi.dulichovietnam.net	40	images.chinabytes.info
4	danang.dulichovietnam.net	41	job.supperpow.com
5	dalat.hanoi.dulichovietnam.net	42	mobile.pagmobiles.info
6	hanoi.hanoi.dulichovietnam.net	43	nsquery.net
7	danang.danang.dulichovietnam.net	44	push.relasign.org
8	dalat.dulichovietnam.net	45	seri.volveri.net
10	danang.dalat.dulichovietnam.net	46	syn.timeizu.net
11	danang.hanoi.dulichovietnam.net	47	tonholding.com
12	dalat.dalat.dulichovietnam.net	48	update-flashs.com
13	hanoi.dalat.dulichovietnam.net	49	vphelp.net
14	dulichovietnam.net	50	24.datatimes.org
15	anh.phimhainhat.net	51	blog.panggin.org
16	data.desvn.org	52	datatimes.org
17	data.phimnoi.org	53	emp.gapte.name
18	dav.thanhmlen.com	54	gl-appspot.org

19	home.phimnoi.org	55	high.vphelp.net
20	home.vietnamplos.com	56	imaps.qki6.com
21	login.phimhainhat.net	57	lighpress.info
22	login.phimnoi.org	58	news.lighpress.info
23	my.phimhainhat.net	59	pagmobiles.info
24	news.phapluats.com	60	relasign.org
25	news.vietnannet.com	61	ssl.zin0.com
26	vietnam.phimhainhat.net	62	teriava.com
27	tulationeva.com	63	img.fanspeed.net
28	vieweva.com	64	menmin.strezf.com
29	yii.yiihao126.net	64	notifieeva.com
30	contay.deaftone.com	65	paidprefund.org
31	docksugs.org	66	share.codehao.net
32	facebook-edn.net	67	static.jg7.org
33	help.checkonl.org	68	timeizu.net
34	icon.torrentart.com	69	untitled.po9z.com
35	volveri.net	70	zone.apize.net
36	desvn.org và các subdomain	71	Phimnoi.org và các subdomain
37	Phimhainhat.net và các subdomain		

III. Danh sách mã băm (HashMD5)

STT	Mã băm – MD5
1	b147314203f74fdda266805cf6f84876
2	3975e3ae679aff3e0d0db5622b6e31a5
3	a64264e872f551b0b0140603293e24e7
4	4965b96bef1353006008d55e178e72b0
5	2eb51010abee4dee8aee5e16f2982e8f
6	b5e473936d325b79d463e9f46602254b
7	e58e41231eeba4952e03038d585eeca3
8	9fab515721ee1123e065497e6e854fd3
9	0f1d8e43863231a3fe86e62894aa48e4
10	ed718baf0ee7284769e8f65dadde8bae
11	7a6180595576542l4a1ba2370a48b887
12	6b44a8f4ded0802a2eb6275d973621b2
13	7a95abdf426144aa5305f1a59247f9aa
14	850172afad42defeb87af969f65759a6
15	e27e1759081284db15da140132bbd79f
16	e27026fdaa4e118b9dac9592a0ea2003
17	4e78b1b95056e188753a8f79b2a41f0f
18	f1a8aadb10a3e5e192b6d06d9699e276
19	58e4d4e0aaefe4e5493243e877bbbe74
20	46e522eba5ee9d837f983206441bbd5b