UBND TỈNH HÀ TĨNH
SỞ VĂN HÓA, THỂ THAO VÀ DU LỊCH

Số: 774 /SVHTTDL-VP
V/v báo cáo giám sát, ngăn chặn khẩn cấp hệ thống máy chủ điều kiển mã độc tấn công có chủ đích APT

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

Hà Tĩnh, ngày 27 tháng 9 năm 2017

Kính gửi: Sở Thông tin và Truyền thông

Thực hiện Công văn số 641/STTTT-CNTT, ngày 18/9/2017 của Sở Thông tin và Truyền thông, về việc giám sát, ngăn chặn khẩn cấp hệ thống máy chủ điều kiển mã độc tấn công có chủ đích APT. Sau khi nghiên cứu Sở Văn hóa, Thể thao và Du lịch đã tiến hành ngăn chặn các địa chỉ IP và tên miền máy chủ điều khiển mã độc *(có phục lục kèm theo)*.

Vậy Sở Văn hóa, Thể thao và Du lịch báo cáo để Sở Thông tin và Truyền thông biết và tổng hợp./.

Nơi nhận:
- Như trên;
- Trung tâm CNTT và Truyền thông Hà Tĩnh
- Giám đốc, các Phó Giám đốc Sở;
- Lưu: VT.

TL.GIÁM ĐỐC
CHÁNH VĂN PHÒNG

Đã ký

Lê Thanh Hải

UBND TỈNH HÀ TĨNH
SỞ VĂN HÓA, THỂ THAO VÀ DU LỊCH

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

PHỤ LỤC BÁO CÁO
Kết quả giảm sát, ngăn chặn khẩn cấp hệ thống máy chủ điều khiển mã độc tấn công có chủ đích APT

(Kèm theo công văn số /SVHTT&DL-VP ngày /9/2017 của Sở VHTT&DL)

1. Thiết bị ngăn chặn kết nối của đơn vị: Firewall Draytek Vigor 2925; Modem Firewall Draytek Vigor 2925

2. Địa chỉ IP và Tên miền máy chủ điều khiển mã độc đã được chặn:

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

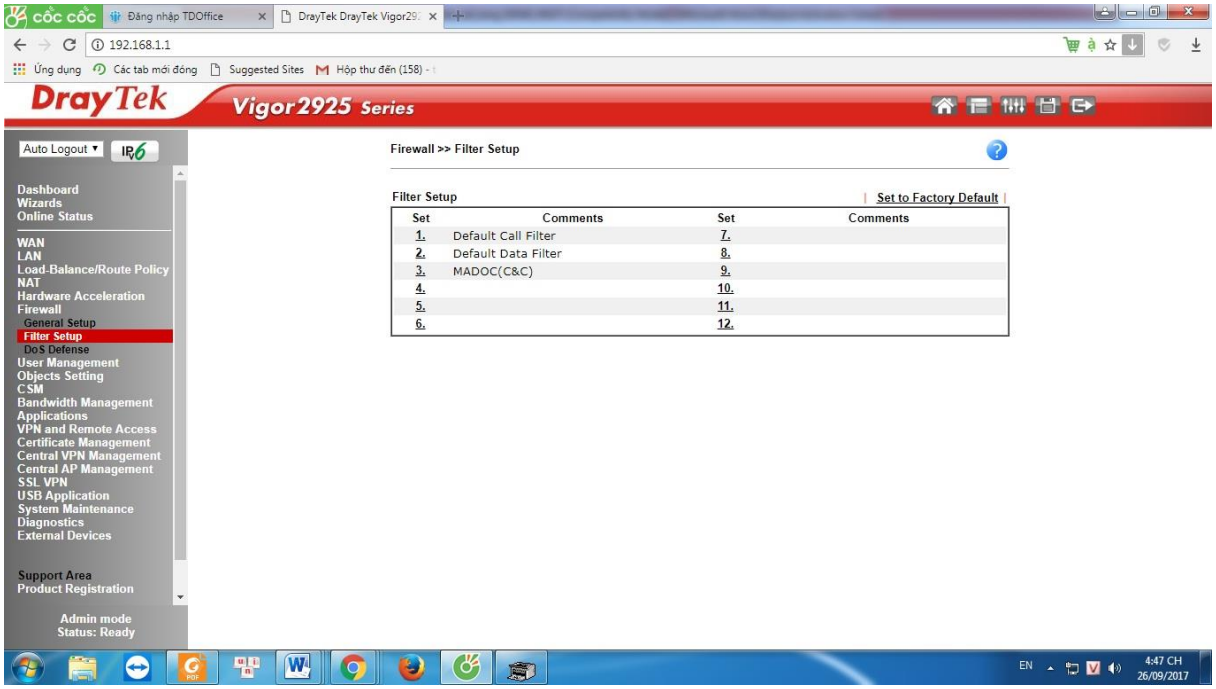
STT	Địachỉ IP C&C	STT	Địachỉ IP C&C
1	209.58.179.202	10	193.169.245.78
2	209.58.176.46	11	104.237.218.72
3	188.42.254.112	12	193.169.245.137
4	66.154.125.145	13	23.227.196.210
6	60.251.29.40	14	185.157.79.3
7	103.53.197.202	15	104.237.218.70
8	58.158.177.102	16	62.210.115.97
9	216.107.152.217	17	176.223.165.165

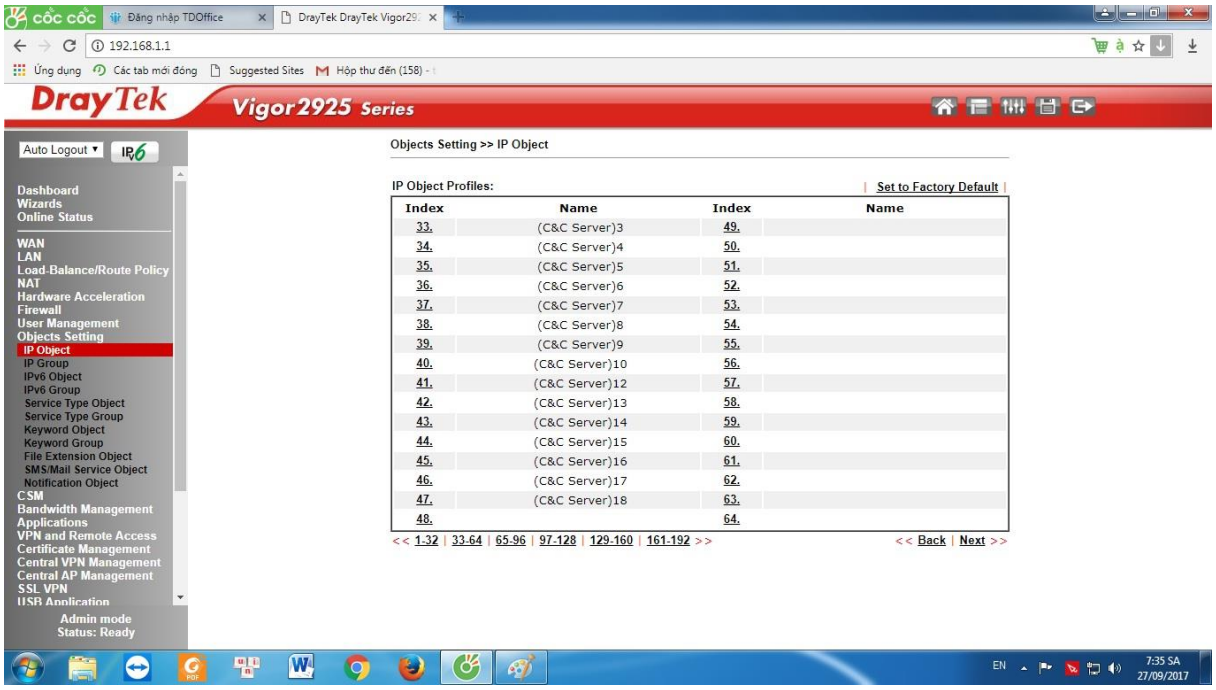
b. Danh sách tên miền máy chủ độc hại (C&C Server)

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.dcsvn.org	52	datatimes.org
17	data.phimnoi.org	53	emp.gapte.name
18	dav.thanhnlen.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	notificeva.com
30	contay.deaftone.com	65	paidprefund.org
31	docksugs.org	66	share.codehao.net
32	facebook-cdn.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	dcsvn.org và các subdomain	71	Phimnoi.org và các subdomain
37	Phimhainhat.net và các subdomain		

3. Hình ảnh chụp màn hình phần cấu hình chặn kết nối của thiết bị





4. Tổng số máy tính của đơn vị: 42;

5. Số máy tính bị nhiễm mã độc: 0;

6. Số máy tính đã được cập nhật các bản vá cho hệ điều hành: 42

7. Số máy tính sử dụng hệ điều hành Windows: 42

8. Số máy tính sử dụng phần mềm Microsoft Office: 60

9. Số máy tính sử dụng phần mềm Microsoft Office có tồn tại lỗ hổng có CVE: CVE-2012-0158, CVE-2017-0199, MS17-010: 0

10. Số máy tính đã được cập nhật các bản vá phần mềm: 0