

UBND TỈNH GIA LAI
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

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

Số: 767/STTTT-CNTT
V/v giám sát, ngăn chặn khẩn cấp hệ thống
máy chủ điều khiển mã độc tấn công
có chủ đích APT

Gia Lai, ngày 12 tháng 9 năm 2017

Kính gửi:

- Văn phòng Tỉnh ủy;
- Văn phòng Hội đồng nhân dân tỉnh;
- Văn phòng Ủy ban Mặt trận tổ quốc Việt Nam tỉnh;
- Công an tỉnh;
- Bộ chỉ huy quân sự tỉnh;
- Các Doanh nghiệp Viễn thông trên địa bàn tỉnh;
- Các Sở, ban, ngành, các hội đoàn thể;
- Ủy ban nhân dân các huyện, thị xã, thành phố.

Sở Thông tin và Truyền thông nhận được Công văn số 298/VNCERT-ĐPƯC ngày 07/9/2017 của Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam (VNCERT) về việc giám sát, ngăn chặn khẩn cấp hệ thống máy chủ điều khiển mã độc tấn công có chủ đích APT. Theo đó, Trung tâm VNCERT thông báo về việc phát hiện ra dấu hiệu chiến dịch tấn công nhằm vào các hệ thống thông tin quan trọng tại Việt Nam thông qua việc phát tán và điều khiển mã độc tấn công có chủ đích (APT). Mã độc này rất tinh vi, chúng có khả năng phát hiện các môi trường phân tích mã độc nhằm tránh bị 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.

Căn cứ nội dung yêu cầu của Trung tâm VNCERT, Sở Thông tin và Truyền thông đề nghị Lãnh đạo các cơ quan, đơn vị thực hiện khẩn cấp các 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 kèm theo;
2. Nếu phát hiện mã độc cần nhanh chóng cô lập vùng/máy và tiến hành điều tra xử lý (cài đặt lại hệ điều hành nếu không gỡ bỏ được triệt để);
3. Cập nhật các bản vá cho hệ điều hành và phần mềm (nhất là Microsoft Office – nếu sử dụng). 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 Đơn vị chuyên trách ứng cứu sự cố an toàn thông tin mạng của tỉnh (Sở Thông tin và Truyền thông) và Cơ quan Điều phối ứng cứu sự cố Quốc Gia (Trung tâm VNCERT) trước ngày 30/9/2017.

Mã độc APT là loại mã độc nguy hiểm, tin tặc có thể tấn công leo thang đặc quyền gây ra hậu quả nghiêm trọng, để đảm bảo an toàn thông tin trên hệ thống do các cơ quan, đơn vị đang quản lý, Sở Thông tin và Truyền thông đề nghị các đơn vị nghiêm túc thực hiện các nội dung nêu trên.

Các cơ quan, đơn vị có thể tải Công văn số 298/VNCERT-ĐPƯC ngày 07/9/2017 tại Trang thông tin điện tử của Sở Thông tin và Truyền thông tại địa chỉ: <http://stttt.gialai.gov.vn> (mục Tin tức – Sự kiện\Tin An toàn thông tin).

Trong quá trình thực hiện, nếu có vướng mắc hoặc cần sự hỗ trợ, đề nghị các cơ quan, đơn vị liên hệ:

Cơ quan Điều phối Quốc gia - Trung tâm VNCERT:

- Địa chỉ: Tầng 5 – Tòa nhà 115 Trần Duy Hưng – Cầu Giấy – Hà Nội;
- Điện thoại: 0436404423 số máy lẻ 112;
- Đường dây nóng: 0869 100 319/ 0934 424 009; Thư điện tử tiếp nhận báo cáo sự số: ir@vncert.gov.vn.

Hoặc Phòng Công nghệ thông tin - Sở Thông tin và Truyền thông:

- Địa chỉ: Số 17 Trần Hưng Đạo, Pleiku, Gia Lai.
- Điện thoại: 0269. 3719653 (gặp đồng chí Nguyễn Thị Ngọc Quyên); Thư điện tử: stttt@gialai.gov.vn.

Sở Thông tin và Truyền thông đề nghị các cơ quan, đơn vị quan tâm thực hiện./.

Nơi nhận:

- Như trên;
- UBND tỉnh (báo cáo);
- Trung tâm CNTT&TT (thực hiện);
- Lưu: VT, P. CNTT.

GIÁM ĐỐC

Nguyễn Ngọc Hùng

PHỤ LỤC :

THÔNG TIN VỀ DOMAIN và IP C&C Server LIÊN QUAN ĐẾN MÃ ĐỘC APT
(Kèm theo Công văn số: /STTTT-CNTT ngày 12/09/2017
của Sở Thông tin và Truyền thông tỉnh Gia Lai)

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

Số TT	Địa chỉ IP C&C	Số TT	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	23.227.196.210
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) :

Số TT	Tên miền	Số TT	Tên miền
1	hanoi.danang.dulichvietnam.net	38	blog.docksugs.org
2	dalat.dulichvietnam.net	39	high.expbas.net
3	hanoi.dulichvietnam.net	40	images.chinabytes.info
4	danang.dulichvietnam.net	41	job.supperpow.com
5	dalat.hanoi.dulichvietnam.net	42	mobile.pagmobiles.info
6	hanoi.hanoi.dulichvietnam.net	43	nsquery.net
7	danang.danang.dulichvietnam.net	44	push.relasign.org
8	dalat.dulichvietnam.net	45	seri.volveri.net
10	danang.dalat.dulichvietnam.net	46	syn.timeizu.net
11	danang.hanoi.dulichvietnam.net	47	tonholding.com
12	dalat.dalat.dulichvietnam.net	48	update-flashes.com
13	hanoi.dalat.dulichvietnam.net	49	vphelp.net
14	dulichvietnam.net	50	24.datatimes.org
15	anh.phimhainhat.net	51	blog.panggin.org
16	data.dcsvn.org	52	datatimes.org

Số TT	Tên miền		Số TT	Tên miền
17	data.phimnoi.org		53	emp.gapte.name
18	dav.thanhnlcn.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		71	Phimnoi.org
37	Phimhainhat.net và các subdomain			

III. Danh sách mã băm (HashMD5):

Số TT	Mã băm – MD5
1	b147314203f74fdda266805cf6f84876
2	3975c3ae679aff3e0d0db5622b6c31a5
3	a64264e872f551b0b0140603293c24c7
4	4965b96bef1353006008d55e178e72b0
5	2cb51010abee4dee8aec5e16f2982e8f
6	b5e473936d325b79d463e9f46602254b
7	e58c41231eeba4952c03038d585ecca3

Số TT	Mã băm – MD5
8	9fab515721ce1123e065497e6c854fd3
9	0f1d8c43863231a3fe86c62894aa48e4
10	cd718baf0ec7284769c8f65dadde8bae
11	7a618059557654214a1ba2370a48b887
12	6b44a8f4dcd0802a2cb6275d97362fb2
13	7a95abdf426144aa5305f1a59247f9aa
14	850172afad42dcfeb87af969f65759a6
15	e27e1759081284db15da140132bbd79f
16	e27026fdaa4c118b9dac9592a0ea2003
17	4e78b1b95056c188753a8f79b2a41f0f
18	f1a8aadb10a3c5c192b6d06d9699c276
19	58c4d4e0aaefe4c5493243c877bbbe74
20	46c522cba5ce9d837f983206441bbd5b