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

Số: 298/VNCERT-ĐPƯC

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

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

Hà Nội, ngày 07 tháng 9 năm 2017

VĂN PHÒNG BHXH VIỆT NAM
CÔNG VĂN ĐẾN Số: 2857
Ngày: 15/9/17
CHUYỂN

KHẨN

Kính gửi:

BẢO HIỂM XÃ HỘI VIỆT NAM
ĐẾN Số: 1176
Ngày: 13/9/2017
Chuyển: CNTT
Lưu hồ sơ số:

- Các đơn vị chuyên trách về CNTT, ATTT của Văn phòng Trung ương Đảng, các Ban của 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, các Tổ chức Tài chính, Ngân hàng;
- Các Doanh nghiệp hạ tầng Internet, Viễn thông, Điện lực, Hàng không, Giao thông Vận tải.

Thực hiện công tác theo dõi các sự cố trên không gian mạng Việt Nam, Trung tâm Ứng cứu khẩn cấp máy tính việt Nam (VNCERT) phát hiện ra dấu hiệu của 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 loại 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 thốngthông tin thông qua các máy chủ điều khiển mã độc (C&C Server) đặt bên ngoài lãnh thổ Việt Nam.

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 lýthực hiện khẩn cấp các công việc 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 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 Cơ quan Điều phối ứng cứu sự cố Quốc gia (Trung tâm VNCERT) trước ngày 30 tháng 9 năm 2017.

Trên đây là loại mã độc nguy hiểm. Tin tặc có thể tấn công leo thang đặc quyền gây ra nhiều hậu quả nghiêm trọng, Trung tâm VNCERT yêu câu Lãnh đạo các đơn vị nghiêm túc thực hiện lệnh điều phối.

Cơ quan Điều phối Quốc gia:

Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam

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: 0869 100 319/0934 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);
- Giám đốc (để b/c);
- PGĐ Nguyễn Khắc Lịch;
- Các phòng, chi nhánh: KTHT, NCPT, TVĐT, CNHCM, CNĐN;
- Lưu VT, ĐPƯC.

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

PHỤ LỤC THÔNG TIN VỀ DOMAIN VÀ IP C&C SERVER LIÊN QUAN ĐẾN MÃ ĐỘC APT

(kèm theo công văn số 298/VNCERT-ĐPƯC ngày 07/09/2017)

I. 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
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)

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		

III. Danh sách mã băm (HashMD5)

STT	Mã băm – MD5
1	b147314203f74fdda266805cf6f84876
2	3975c3ae679aff3e0d0db5622b6c31a5
3	a64264e872f551b0b0140603293c24c7
4	4965b96bef1353006008d55e178c72b0
5	2cb51010abee4dee8aec5e16f2982e8f
6	b5e473936d325b79d463e9f46602254b
7	e58c41231eeba4952c03038d585ecca3
8	9fab515721ce1123e065497e6c854fd3
9	0f1d8c43863231a3fe86c62894aa48e4
10	cd718baf0ec7284769c8f65dadde8bae
11	7a6180595576542l4a1ba2370a48b887
12	6b44a8f4dcd0802a2cb6275d97362fb2
13	7a95abdf426144aa5305f1a59247f9aa
14	850172afad42dcfeb87af969f65759a6
15	e27e1759081284db15da140132bbd79f
16	e27026fdaa4c118b9dac9592a0ea2003
17	4e78b1b95056c188753a8f79b2a41f0f
18	f1a8aadb10a3c5c192b6d06d9699c276
19	58c4d4e0aaefe4c5493243c877bbbe74
20	46c522cba5ce9d837f983206441bbd5b