BỘ THÔNG TIN TRUYỀN THÔNG
CỤC AN TOÀN THÔNG TIN

Số: 941 /CATTT-NCSC
V/v rà soát, ngăn chặn nguy cơ tấn công APT

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

Hà Nội, ngày 27 tháng 06 năm 2022

Kính gửi:

- Đơn vị chuyên trách về CNTT các Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ;
- Sở Thông tin và Truyền thông các tỉnh, thành phố trực thuộc Trung ương;
- Các Tập đoàn, Tổng công ty nhà nước; các Ngân hàng TMCP; các tổ chức tài chính;
- Hệ thống các đơn vị chuyên trách về an toàn thông tin.

Qua công tác giám sát an toàn trên không gian mạng và hoạt động hợp tác, chia sẻ thông tin với các tổ chức lớn về an toàn thông tin trong và ngoài nước, Cục An toàn thông tin phát hiện thời gian gần đây, nhiều nhóm tấn công có chủ đích (APT) đang tích cực hoạt động, để thực hiện tấn công vào hệ thống thông tin của nhiều quốc gia trên thế giới, trong đó có Việt Nam.

Với kết quả thống kê sơ bộ, trong 06 tháng đầu năm 2022 vừa qua Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC) phát hiện có nhiều nhóm tấn công APT đang mở rộng hạ tầng điều khiển để triển khai các hoạt động tấn công, nổi bật như nhóm **Aoqin Dragon, Stone Panda, Mustang Panda, Lazarus.**

Thông tin danh sách chi tiết về IoC của các nhóm tấn công APT này có tại phụ lục kèm theo.

Theo nhận định của Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC), tấn công APT tại Việt Nam đang ngày càng gia tăng cả về số lượng và mức độ tinh vi, bao gồm việc thường xuyên khai thác các lỗ hổng bảo mật chưa được vá trong các chiến dịch tấn công (như lỗ hổng Log4j, lỗ hổng trong sản phẩm Vmware, Exchange Server,…).

Nhằm hạn chế, ngăn chặn, xử lý sớm các nguy cơ tấn công APT vào hệ thống thông tin của các cơ quan, tổ chức tại Việt Nam, Cục An toàn thông tin đề nghị Quý đơn vị thực hiện:

1. Rà soát, giám sát và thống kê kết nối đến các địa chỉ IP/tên miền độc hại. Báo cáo về Cục An toàn thông tin trong trường hợp phát hiện có kết nối đến các địa chỉ độc hại này.

2. Ngăn chặn toàn bộ kết nối đến và đi liên quan đến các địa chỉ IP/tên miền độc hại này.

3. Trong trường hợp cần thiết có thể liên hệ đầu mối hỗ trợ của Cục An toàn thông tin: Trung tâm Giám sát an toàn không gian mạng quốc gia, điện thoại 02432091616, thư điện tử: ais@mic.gov.vn.

Trân trọng./.

Nơi nhận:
- Như trên;
- Bộ trưởng (để b/c);
- Thứ trưởng Nguyễn Huy Dũng (để b/c);
- Cục A05, Bộ Công an;
- Bộ Tư lệnh 86, Bộ Quốc phòng;
- Ban Cơ yếu Chính phủ;
- Cục trưởng;
- Trung tâm VNCERT/CC, phòng ATHTTT;
- Lưu: VT, NCSC.

CỤC TRƯỞNG

CỘNG HÒA X.H.C.N VIỆT NAM
CỤC AN TOÀN THÔNG TIN
BỘ THÔNG TIN VÀ TRUYỀN THÔNG

Nguyễn Thành Phúc

Phụ lục
Thông tin IoC liên quan đến các nhóm APT
(Kèm theo Công văn số /CATTT-NCSC ngày / /2022 của Cục An toàn thông tin)

Tên nhóm APT	Ip/Domain độc hại	Ip/Domain độc hại
Aoqin Dragon	cvb[.]hotcup[.]pw dns[.]foodforthought1[.]com test[.]facebookmap[.]top 45[.]77[.]11[.]148 back[.]satunusa[.]org baomoi[.]vnptnet[.]info bbw[.]fushing[.]org bca[.]zdungk[.]com bkav[.]manlish[.]net bkav[.]welikejack[.]com bkavonline[.]vnptnet[.]info bush2015[.]net cl[.]weststations[.]com cloundvietnam[.]com cpt[.]vnptnet[.]inf dns[.]lioncity[.]top dns[.]satunusa[.]org dns[.]zdungk[.]com ds[.]vdcvn[.]com ds[.]xrayccc[.]top facebookmap[.]top fbcl2[.]adsoft[.]name fbcl2[.]softad[.]net flower2[.]yyppmm[.]com game[.]vietnamflash[.]com hello[.]bluesky1234[.]com ipad[.]vnptnet[.]info ks[.]manlish[.]net lepad[.]fushing[.]org lllyyy[.]adsoft[.]name lucky[.]manlish[.]net	sky[.]vietnamflash[.]com tcv[.]tiger1234[.]com telecom[.]longvn[.]net telecom[.]manlish[.]net th-y3[.]adsoft[.]name th550[.]adsoft[.]name th550[.]softad[.]net three[.]welikejack[.]com thy3[.]softad[.]net vdcvn[.]com video[.]philstar2[.]com viet[.]vnptnet[.]info viet[.]zdungk[.]com vietnam[.]vnptnet[.]info vietnamflash[.]com vnet[.]fushing[.]org vnn[.]bush2015[.]net vnn[.]phung123[.]com webmail[.]philstar2[.]com www[.]bush2015[.]net yok[.]fushing[.]org yote[.]dellyou[.]com zing[.]vietnamflash[.]com zingme[.]dungk[.]com zingme[.]longvn[.]net zw[.]dinhk[.]net zw[.]phung123[.]com mobile[.]vdcvn[.]com moit[.]longvn[.]net movie[.]vdcvn[.]com news[.]philstar2[.]com

	ma550[.]adsoft[.]name ma550[.]softad[.]net mail[.]comnnet[.]net mail[.]tiger1234[.]com mail[.]vdcvn[.]com mass[.]longvn[.]net mcafee[.]bluesky1234[.]com media[.]vietnamflash[.]com mil[.]dungk[.]com mil[.]zdungk[.]com mmchj2[.]telorg[.]net	news[.]welikejack[.]com npt[.]vnptnet[.]info ns[.]fushing[.]org nycl[.]neverdropd[.]com phcl[.]followag[.]org phcl[.]neverdropd[.]com pna[.]adsoft[.]name pnavy3[.]neverdropd[.]com sky[.]bush2015[.]net mmslsh[.]tiger1234[.]com
Stone Panda	v5[.]hinitial[.]com v4[.]hinitial[.]com v3[.]hinitial[.]com v2[.]hinitial[.]com jack[.]micfkbeljacob[.]com df[.]micfkbeljacob[.]com micfkbeljacob[.]com	t1[.]hinitial[.]com mailedc[.]publicvm[.]com helpinfo[.]publicvm[.]com goodluck23[.]jp[.]us goodjob36[.]publicvm[.]com hinitial[.]com 61[.]221[.]66[.]85
Mustang Panda	images[.]myanmarnewsonline[.]org update[.]hilifimyanmar[.]com download[.]hilifimyanmar[.]com	myanmarnewsonline[.]org hilifimyanmar[.]com 45[.]134[.]83[.]4 154[.]204[.]27[.]130 154[.]204[.]26[.]120 45[.]134[.]83[.]4 154[.]204[.]26[.]120
Lazarus	66[.]154[.]102[.]91 onlinestockwatch[.]net mail[.]usengineergroup[.]com usengineergroup[.]com 109[.]248[.]144[.]155 109[.]248[.]144[.]155 109[.]248[.]144[.]136 45[.]57[.]245[.]17 193[.]56[.]28[.]32 alticgo[.]com it[.]zvc[.]capital cloud[.]beenos[.]biz zvc[.]capital	155[.]94[.]210[.]11 109[.]248[.]144[.]155 tokenais[.]com esilet[.]com dafom[.]dev cryptais[.]com aumentarelevisite[.]com 15[.]235[.]33[.]14 junepr happy[.]nanoace[.]co[.]kr mariamchurch[.]com jungfrau[.]co[.]kr int[.]com

	beenos[.]biz ric-camid[.]re[.]kr	

Ghi chú: Đây là danh sách một số nhóm tấn công APT có hoạt động nổi bật trong thời gian gần đây. Thông tin về các nhóm tấn công APT khác được chia sẻ trên hệ thống MISP của Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC) tại: https://misp.ais.gov.vn.