UBND TỈNH HÀ NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

Số: 712 /STTTT-BCVTCNTT

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 Nam, ngày 28 tháng 6 năm 2022

Kính gửi:

- Văn phòng Tỉnh ủy Hà Nam;
- Các sở, ban, ngành, cơ quan, đoàn thể của tỉnh;
- UBND các huyện, thị xã, thành phố.

Căn cứ Công văn số 941/CATTT-NCSC ngày 27/6/2022 của Cục An toàn thông tin, Bộ Thông tin và Truyền thông về việc rà soát, ngăn chặn nguy cơ tấn công APT;

Qua công tác giám sát an toàn trên không gian mạng, 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. Trong 06 tháng đầu năm 2022, 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 tại phụ lục kèm theo)*.

Nhằm tăng cường công tác bảo đảm an toàn, an ninh thông tin, đặc biệt là bảo vệ các hệ thống thông tin của các cơ quan, đơn vị trên địa bàn tỉnh, Sở Thông tin và Truyền thông đề nghị các cơ quan, đơn vị:

- Rà soát, giám sát và thống kê kết nối đến các địa chỉ IP/tên miền độc hại trên, báo cáo về Sở Thông tin và Truyền thông trong trường hợp phát hiện có kết nối đến các địa chỉ độc hại trên.

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

Đầu mối liên hệ, hỗ trợ:

- Sở Thông tin và Truyền thông (Trung tâm Công nghệ thông tin và Truyền thông - Bộ phận thường trực Đội Ứng cứu sự cố an toàn thông tin mạng tỉnh Hà Nam). Điện thoại: **0226.3846333**. Email: **ttcntt@hanam.gov.vn**

- Trung tâm Giám sát an toàn thông tin mạng quốc gia (NCSC), Cục An toàn thông tin. Điện thoại di động: **0243.2091616**. Email: **ais@mic.gov.vn**./.

Nơi nhận:
- Như trên;
- Lưu VT.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HÒA XHCN VIỆT NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
TỈNH HÀ NAM

Nguyễn Đức Cường

Phụ lục
THÔNG TIN IOC LIÊN QUAN ĐẾN CÁC NHÓM APT

(Kèm theo Công văn số /STTTT-BCVTCNTT ngày / /2022 của Sở Thông tin và Truyền thông Hà Nam)

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	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

Tên nhóm APT	IP/Domain độc hại	IP/Domain độc hại
	hello[.]bluesky1234[.]com ipad[.]vnptnet[.]info ks[.]manlish[.]net lepad[.]fushing[.]org lllyyy[.]adsoft[.]name lucky[.]manlish[.]net 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	zw[.]dinhk[.]net zw[.]phung123[.]com mobile[.]vdcvn[.]com moit[.]longvn[.]net movie[.]vdcvn[.]com news[.]philstar2[.]com 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	myanmarnewsonline[.]org hilifimyanmar[.]com 45[.]134[.]83[.]4

Tên nhóm APT	IP/Domain độc hại	IP/Domain độc hại
	download[.]hilifimyanmar[.]com	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 beenos[.]biz ric-camid[.]re[.]kr	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

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.