ỦY BAN NHÂN DÂN HUYỆN THẠCH THÀNH	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập – Tự do – Hạnh phúc
Số: 2214 /UBND-VHTT V/v rà soát, ngăn chặn nguy cơ tấn công có chủ đích (APT).	*Thạch Thành, ngày 28 tháng 7 năm 2022*

Kính gửi:
- Các phòng, ban, cơ quan, đơn vị cấp huyện;
- Các tổ chức đoàn thể chính trị cấp huyện;
- Các doanh nghiệp viễn thông, CNTT trên địa bàn huyện;
- UBND các xã, thị trấn.

Thực hiện Công văn số: 93/TTCNTT&TT-QTHT, ngày 11/7/2022 của Trung tâm công nghệ thông tin và truyền thông Thanh Hóa về rà soát, ngăn chặn nguy cơ tấn công có chủ đích (APT). Theo đó, 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, nổi bật như nhóm ***Aoqin Dragon, Stone Panda, Mustang Panda, Lazarus***, để thực hiện tấn công vào hệ thống thông tin của nhiều quốc gia trên thế giới, trong đó có Việt Nam.

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,…).

Để tăng cường chủ động phòng ngừa các rủi ro mất an toàn thông tin tại các hệ thống thông tin của các cơ quan, tổ chức và doanh nghiệp do các hình thức tấn công trên có thể xảy ra, UBND huyện Thạch Thành đề nghị các cơ quan, đơn vị chỉ đạo các bộ phận, cá nhân thực hiện những nội dung sau:

1. Tăng cường giám sát và sẵn sàng phương án xử lý khi phát hiện có dấu hiệu bị khai thác, tấn công mạng; đồng thời thường xuyên theo dõi kênh cảnh báo của các cơ quan chức năng và các tổ chức lớn về an toàn thông tin để phát hiện kịp thời các nguy cơ tấn công mạng.

2. Các doanh nghiệp viễn thông, CNTT, Văn phòng HĐND&UBND huyện: Phân công cán bộ phụ trách, phối hợp với Trung tâm công nghệ thông tin và truyền thông Thanh Hóa thực hiện rà soát, giám sát và ngăn chặn toàn bộ kết nối đến và đi liên quan đến các địa chỉ IP/tên miền độc hại của các nhóm tấn công trên *(danh sách tại Phụ lục kèm theo).* Tăng cường giám sát, kịp thời phát hiện các kết nối đến các địa chỉ độc hại này để phối hợp xử lý.

Hướng dẫn kỹ thuật cách thức thực hiện chi tiết việc ngăn chặn các kết nối trên tại địa chỉ: https://attt.thanhhoa.gov.vn

Trong quá trình thực hiện, nếu gặp khó khăn, vướng mắc về kỹ thuật liên quan đến các nội dung, công việc trên đề nghị liên hệ với Trung tâm Công nghệ thông tin và Truyền thông Thanh Hóa, điện thoại: (0237)3718.699 hoặc cán bộ quản trị mạng của UBND huyện (đ/c Trương Lê Hiển, ĐT: 098.1616.123) để phối hợp hỗ trợ, xử lý.

Đề nghị các phòng, ban, cơ quan, đơn vị, doanh nghiệp triển khai thực hiện tốt các nội dung trên./.

Nơi nhận:
- Như trên;
- Chủ tịch, các PCT UBND huyện;
- Lưu: VT, VHTT.

KT. CHỦ TỊCH
PHÓ CHỦ TỊCH

Nguyễn Đình Tam

Phụ lục: Thông tin danh sách tên miền/IP về các nhóm tấn công APT
(Kèm theo công văn số /UBND-VHTT ngày /7/2022 của UBND huyện Thạch Thành)

1. Danh sách tên miền/IP

TT	Tên nhóm APT	Ip/Domain độc hại	
1	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 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	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 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
2	Stone	v5[.]hinitial[.]com	t1[.]hinitial[.]com

	Panda	v4[.]hinitial[.]com v3[.]hinitial[.]com v2[.]hinitial[.]com jack[.]micfkbeljacob[.]com df[.]micfkbeljacob[.]com micfkbeljacob[.]com	mailedc[.]publicvm[.]com helpinfo[.]publicvm[.]com goodluck23[.]jp[.]us goodjob36[.]publicvm[.]com hinitial[.]com 61[.]221[.]66[.]85
3	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
4	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

2. Hướng dẫn khắc phục

Hướng dẫn chi tiết khắc phục các lỗ hổng bảo mật trên tại địa chỉ: https://attt.thanhhoa.gov.vn *(Kỹ năng An toàn thông tin -> Mục Hướng dẫn)*