BỘ KHOA HỌC VÀ CÔNG NGHỆ
TRUNG TÂM CÔNG NGHỆ THÔNG TIN

Số: 228/TTCNTT-KTHT
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 29 tháng 06 năm 2022

Kính gửi: Các đơn vị trực thuộc Bộ có hệ thống 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 – Bộ Thông tin và Truyền thông 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 Cục An toàn thông tin 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 Cục An toàn thông tin, 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, Trung tâm Công nghệ 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 Trung tâm Công nghệ 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.

Trong trường hợp cần thiết, Quý đơn vị liên hệ đầu mối hỗ trợ của Trung tâm Công nghệ thông tin: Phòng Kỹ thuật hạ tầng, điện thoại 024.39439060, thư điện tử: phongktht@most.gov.vn.

Trân trọng./.

Nơi nhận:
- Như trên;
- Thứ trưởng Bùi Thế Duy (để b/c);
- Cổng thông tin điện tử Bộ KH&CN;
- Lưu: VT, KTHT.

GIÁM ĐỐC

BỘ KHOA HỌC VÀ CÔNG NGHỆ
TRUNG TÂM CÔNG NGHỆ THÔNG TIN

Hà Quốc Trung

Phụ lục
Thông tin IoC liên quan đến các nhóm APT
(Kèm theo Công văn số 228 /TTCNTT-KTHT ngày 29 /06 /2022 của Trung tâm Công nghệ thông tin)

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

	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	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 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	155.94.210.11 109.248.144.155 tokenais.com esilet.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	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.

DANH SÁCH CÁC ĐƠN VỊ NHẬN VĂN BẢN

(Kèm theo Công văn số 228 /TTCNTT-KTHT ngày 29 /06 /2022 của Trung tâm Công nghệ thông tin)

TT	Tên đơn vị
1.	Thanh tra Bộ
2.	Cục Công tác phía Nam
3.	Cục Ứng dụng và phát triển công nghệ
4.	Cục Năng lượng nguyên tử
5.	Cục Thông tin Khoa học và Công nghệ Quốc gia
6.	Cục Phát triển thị trường và doanh nghiệp khoa học và công nghệ
7.	Cục An toàn bức xạ và hạt nhân
8.	Cục Sở hữu trí tuệ
9.	Tổng cục Tiêu chuẩn Đo lường Chất lượng
10.	Ban quản lý khu công nghệ cao Hoà Lạc
11.	Học viện Khoa học, Công nghệ và Đổi mới sáng tạo
12.	Viện Khoa học và công nghệ Việt Nam - Hàn Quốc (VKIST)
13.	Viện Nghiên cứu sáng chế và Khai thác công nghệ
14.	Viện Năng lượng nguyên tử Việt Nam
15.	Viện Ứng dụng công nghệ
16.	Viện Đánh giá khoa học và Định giá công nghệ
17.	Viện Khoa học sở hữu trí tuệ
18.	Viện Nghiên cứu và Phát triển Vùng
19.	Văn phòng các Chương trình trọng điểm cấp nhà nước
20.	Văn phòng Công nhận chất lượng
21.	Văn phòng Đăng ký hoạt động khoa học và công nghệ
22.	Văn phòng các Chương trình khoa học và công nghệ quốc gia
23.	Báo điện tử Tin nhanh Việt Nam (VnExpress)
24.	Tạp chí Khoa học và Công nghệ Việt Nam
25.	Nhà xuất bản Khoa học và Kỹ thuật
26.	Quỹ Phát triển khoa học và công nghệ quốc gia
27.	Quỹ Đổi mới công nghệ quốc gia
28.	Trung tâm Nghiên cứu và Phát triển truyền thông khoa học và công nghệ
29.	Trung tâm Nghiên cứu và Phát triển hội nhập khoa học và công nghệ quốc tế