UỶ BAN NHÂN DÂN **HUYỆN QUỲ HỢP**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 1576 /UBND-VH V/v cảnh báo chiến dịch tấn công của nhóm APT "MirrorFace"	*Quỳ Hợp, ngày 12 tháng 8 năm 2024*

Kính gửi:
- Trưởng các phòng, ngành, đoàn thể cấp huyện;
- Chủ tịch UBND các xã, thị trấn;
- Thủ trưởng các cơ quan, đơn vị trên địa bàn huyện;
- VNPT Quỳ Hợp.

Thực hiện Công văn số 1577/STTTT-CĐS ngày 07/8/2024 của Sở Thông tin và Truyền thông tỉnh Nghệ An về việc *"Cảnh báo chiến dịch tấn công của nhóm APT "MirrorFace"*.

Ngày 06/08/2024, Cục An toàn thông tin đã ban hành công văn số 1543/CATTT-NCSC về việc cảnh báo chiến dịch tấn công của nhóm APT "MirrorFace". Theo văn bản này, qua theo dõi, giám sát không gian mạng, Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC), thuộc Cục An toàn thông tin - Bộ Thông tin và Truyền thông, đã phát hiện và ghi nhận các thông tin liên quan đến chiến dịch tấn công mạng được thực hiện bởi nhóm tấn công APT MirrorFace. Mục tiêu của nhóm MirrorFace là các tổ chức chính trị, các viện nghiên cứu, nhà sản xuất (*thông tin chi tiết xem tại Phụ lục kèm theo*).

Thực hiện chức năng quản lý nhà nước về an toàn thông tin mạng, Ủy ban nhân dân huyện đề nghị các phòng, ngành cấp huyện, UBND các xã, thị trấn, các cơ quan, đơn vị trên địa bàn huyện chỉ đạo triển khai thực hiện các nhiệm vụ chính như sau:

1. Một số giải pháp cần triển khai:

- Kiểm tra, rà soát hệ thống thông tin đang sử dụng có khả năng bị ảnh hưởng bởi chiến dịch tấn công trên. Chủ động theo dõi các thông tin liên quan đến đến chiến dịch nhằm thực hiện ngăn chặn nhằm tránh nguy cơ bị tấn công.

- 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. Phòng Văn hóa và Thông tin huyện:

Đăng tải toàn văn nội dung công văn số công văn số 1543/CATTT-NCSC ngày 06/08/2024 của Cục An toàn thông tin về việc về việc cảnh báo chiến dịch tấn công của nhóm APT "MirrorFace" lên Cổng thông tin điện tử huyện Quỳ Hợp.

3. VNPT Quỳ Hợp:

Đề nghị VNPT Quỳ Hợp tuân thủ các quy định pháp lý hiện hành và các điều

khoản thuộc hợp đồng thuê dịch vụ có liên quan đến công tác an toàn thông tin để đảm bảo hoạt động ổn định, an toàn các hệ thống thông tin hiện đang cung cấp dịch vụ trên địa bàn huyện.

Trong quá trình thực hiện, nếu có khó khăn vướng mắc hoặc trường hợp cần hỗ trợ giám sát, xử lý, ứng cứu sự cố đề nghị liên hệ thông qua các đầu mối:

- Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam (VNCERT/CC), điện thoại 024.3640.4421 hoặc số điện thoại trực đường dây nóng ứng cứu sự cố 086.9100.317, thư điện tử: ir@vncert.vn.

- Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC), điện thoại: 024.32091.616 hoặc số điện thoại trực đường dây nóng hỗ trợ giám sát, cảnh báo sớm 038.9942.878, thư điện tử: ais@mic.gov.vn.

- Phòng An toàn hệ thống thông tin, Cục An toàn thông tin (hướng dẫn công tác bảo đảm an toàn hệ thống thông tin theo cấp độ), điện thoại: 0369596886, thư điện tử: athttt@mic.gov.vn.

- Đội Ứng cứu sự cố an toàn thông tin mạng tỉnh Nghệ An, điện thoại: 02383.500027

UBND huyện yêu cầu các phòng, ngành cấp huyện, UBND các xã, thị trấn, các cơ quan, đơn vị trên địa bàn huyện triển khai thực hiện nghiêm túc./.

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

TM. UỶ BAN NHÂN DÂN
KT. CHỦ TỊCH
PHÓ CHỦ TỊCH

ỦY BAN NHÂN DÂN HUYỆN QUỲ HỢP T. NGHỆ AN

Hoàng Văn Thái

Phụ lục

THÔNG TIN CHI TIẾT VỀ LỖ HỔNG AN TOÀN THÔNG TIN

(Kèm theo Công văn số 1576/UBND-VH ngày 12/8/2024 của UBND huyện)

1. Thông tin chi tiết về chiến dịch tấn công của nhóm APT "MirrorFace"

Gần đây, đã phát hiện và ghi nhận chiến dịch tấn công trên không gian mạng của nhóm tấn công MirrorFace nhằm vào các tổ chức tài chính, viện nghiện cứu và nhà sản xuất. Nhóm đã thực hiện khai thác các lỗ hổng an toàn thông tin trên sản phẩm Array AG và FortiGate nhằm phát tán mã độc NOOPDOOR.

Mã độc NOOPDOOR là một shellcode được gài vào ứng dụng hợp pháp trên hệ thống và có hai biến thể dưới dạng file .XML và .DLL. Cả hai biến thể này chỉ khác về bước xâm nhập và giống nhau về chức năng, cho phép nhóm MirrorFace thiết lập kết nối thông qua cổng 443, cổng 47000 để tải xuống file, thực thi câu lệnh,…

Sau khi phát tán mã độc trong chiến dịch tấn công, nhóm này thực hiện các hành trái phép như: truy cập vào nơi lưu trữ thông tin xác thực của hệ thống mạng, phát tán mã độc tới các thiết bị khác trong mạng cục bộ; thực hiện các hành vi theo dõi, trích xuất thông tin người dùng. Ngoài ra, MirrorFace còn sử dụng công cụ GO Simple Tunnel trong chiến dịch. Để tránh bị phát hiện, nhóm đối tượng đã khai thác MSBuild để thực thi file .XML chứa mã độc; ghi đè dữ liệu độc hại lên registry của file; chỉnh sửa timestamp; thêm luật vào tường lửa hệ thống để cho phép mã độc được kết nối tới các cổng nhất định; ẩn đi các dịch vụ được kích hoạt; xóa đi ghi chép của Windows Event; xóa file mã độc sau khi khai thác. Chiến dịch sử dụng kỹ thuật DLL side-loading và khai thác MSBuild để thực thi mã độc trên hệ thống.

Các đơn vị có thể tải xuống các mã IOC tại: https://alert.khonggianmang.vn/

Dưới đây là một số IoC liên quan đến các tấn công gần đây

45[.]66[.]217[.]106	89[.]233[.]109[.]69
45[.]77[.]12[.]212	108[.]160[.]130[.]45
207[.]148[.]97[.]235	95[.]85[.]91[.]15
64[.]176[.]214[.]51	168[.]100[.]8[.]103
45[.]76[.]222[.]130	45[.]77[.]183[.]161
207[.]148[.]90[.]45	207[.]148[.]103[.]42
103[.]143[.]208[.]115	103[.]143[.]208[.]29
103[.]143[.]209[.]36	146[.]70[.]79[.]68
91[.]245[.]255[.]30	91[.]245[.]255[.]79
www[.]lookpumrron[.]com	www[.]morrowadded[.]com
minggamevies[.]com	2001:19f0:7001:2ae2:5400:4ff:fe0a:5566
2a12:a300:3600::31b5:2e02	2a12:a300:3700::5d9f:b451
2400:8902::f03c:93ff:fe8a:5327	bcd34d436cbac235b56ee5b7273baed62bf385ee13721c7fdcfc00af9ed63997

93af6afb47f4c42bc0da3eedc6ecb9054134f4a47ef0add0d2854049840111072	4f932d6e21fdd0072aba61203c7319693e490adb d9e93a49b0fe870d4d0aed71
43349c97b59d8ba8e1147f911797220b1b7b87609fe4aaa7f1dbacc2c27b361d	9590646b32fec3aafd6c648f69ca9857fb4be2adfabf3bcaf321c8cd25ba7b83
0d59734bdb0e6f4fe6a44312a2d55145e98b00f75a148394b2e4b86436c32f4c	7a7e7e0d817042e54129697947dfb423b607692f4457163b5c62ffea69a8108d
572f6b98cc133b2d0c8a4fd8ff9d14ae36cdaa119086a5d56079354e49d2a7ce	b07c7dfb3617cd40edc1ab309a68489a3aa4aa1e8fd486d047c155c952dc509e
5e7cd0461817b390cf05a7c874e017e9f44eef41e053da99b479a4dfa3a04512	0

2. Tài liệu tham khảo

https://blogs.jpcert.or.jp/en/2024/07/mirrorface-attack-against-japaneseorganisations.html