UBND TỈNH ĐỒNG NAI
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

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

Số: 2698 /STTTT-CĐS
V/v cảnh báo chiến dịch tấn công của nhóm APT "MirrorFace".

Đồng Nai, ngày 15 tháng 8 năm 2024

Kính gửi:
- Các cơ quan Đảng, Nhà nước trên địa bàn tỉnh;
- Các tổ chức chính trị - xã hội trên địa bàn tỉnh;
- Ủy ban Mặt trận Tổ quốc Việt Nam tỉnh;
- Công an tỉnh.

Sở Thông tin và Truyền thông nhận được văn bản số 1543/CATTTT-NCSC ngày 06/8/2024 của Cục An toàn Thông tin về việc cảnh báo chiến dịch tấn công của nhóm APT "MirrorFace". Trong đó, ghi nhận mục tiêu tấn công của nhóm MirrorFace là các tổ chức chính trị, các viện nghiên cứu, nhà sản xuất.

(Thông tin chi tiết xem tại Phụ lục đính kèm)

Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin của Quý đơn vị, của tỉnh và góp phần bảo đảm an toàn cho không gian mạng Việt Nam, Sở Thông tin và Truyền thông khuyến nghị Quý đơn vị thực hiện:

1. 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 chiến dịch nhằm thực hiện ngăn chặn nhằm tránh nguy cơ bị tấn công.

2. 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.

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 0243.2091.616, thư điện tử: ncsc@ais.gov.vn hoặc Sở Thông tin và Truyền thông, điện thoại 0251.3810.269, thư điện tử: attt@dongnai.gov.vn./.

Nơi nhận:
- Như trên;
- Ban Giám đốc Sở;
- TT. CNTT tỉnh (để triển khai);
- Lưu: VT, CĐS, Hùng.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
TỈNH ĐỒNG NAI

Võ Hoàng Khai

Phụ lục
THÔNG TIN CHI TIẾT VỀ CHIẾN DỊCH TẤN CÔNG
(Kèm theo Công văn số 2698 /STTTT-CĐS ngày 15 /8/2024 của Sở Thông tin và Truyền thông)

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
93af6afb47f4c42bc0da3eedc6ecb9054134f4a47ef0add0d285404984011072	4f932d6e21fdd0072aba61203c7319693e490adbd9e93a49b0fe870d4d0aed71
43349c97b59d8ba8e1147f911797220b1b7b87609fe4aaa7f1dbacc2c27b361d	9590646b32fec3aafd6c648f69ca9857fb4be2adfabf3bcaf321c8cd25ba7b83
0d59734bdb0e6f4fe6a44312a2d55145e98b00f75a148394b2e4b86436c32f4c	7a7e7e0d817042e54129697947dfb423b607692f4457163b5c62ffea69a8108d
572f6b98cc133b2d0c8a4fd8ff9d14ae36cdaa119086a5d56079354e49d2a7ce	b07c7dfb3617cd40edc1ab309a68489a3aa4aa1e8fd486d047c155c952dc509e
5e7cd0461817b390cf05a7c874e017e9f44eef41e053da99b479a4dfa3a04512	0

2. Tài liệu tham khảo

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