UBND TỈNH THỪA THIÊN HUẾ
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập – Tự do – Hạnh Phúc

Số: 1716 /STTTT-IOC
V/v cảnh báo nhóm APT "Mustang Panda" thực hiện chiến dịch tấn công nhằm vào Việt Nam

Thừa Thiên Huế, ngày 18 tháng 6 năm 2024

Kính gửi:
- Văn phòng Tỉnh ủy;
- Các cơ quan chuyên môn thuộc UBND tỉnh;
- Các đơn vị sự nghiệp thuộc tỉnh;
- UBND các huyện, thị xã và thành phố Huế;
- Các cơ quan, đơn vị, tổ chức khác có kết kết mạng WAN;
- Đại học Huế

Sở Thông tin và Truyền thông nhận được Công văn số 1095/CATTT-NCSC ngày 14/6/2024 của Cục An toàn thông tin - Bộ Thông tin và Truyền thông về việc cảnh báo nhóm APT "Mustang Panda" thực hiện chiến dịch tấn công nhằm vào Việt Nam.

Trong quá trình giám sát an toàn thông tin trên 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 nhằm vào Việt Nam được thực hiện bởi nhóm tấn công APT "Mustang Panda". Chiến dịch tấn công lần này của nhóm Mustang Panda sử dụng các mồi nhử xoay quanh lĩnh vực giáo dục và thuế, áp dụng nhiều góc tiếp cận, lợi dụng các công cụ như "forfiles.exe" để thực thi file độc hại được lưu ở máy chủ C&C. Ngoài ra, nhóm này còn sử dụng PowerShell, VBScript và các file batch trong chiến dịch tấn công. Mục tiêu mà nhóm hướng tới là các tổ chức chính phủ, tổ chức phi lợi nhuận, tổ chức giáo dục,…

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

Nhằm đảm bảo an toàn thông tin cho các hệ thống thông tin, hệ thống mạng diện rộng của tỉnh, góp phần bảo đảm an toàn cho không gian mạng Việt Nam, Sở Thông tin và Truyền thông đề nghị quý đơn vị chủ động thực hiện các biện pháp sau:

1. Triển khai 02 giải pháp đảm bảo an toàn thông tin cho 100% các máy tính tại đơn vị: Giải pháp phòng, chống mã độc tập trung Bkav Endpoint tại Công văn số 639/STTTT-IOC ngày 29/3/2022; Giải pháp phát hiện và chống tấn công có chủ đích Viettel Endpoint tại Công văn số 1660/STTTT-IOC ngày 22/7/2022 của Sở TTTT;

2. Chú ý cảnh giác thư điện tử không rõ nguồn gốc, thư có các liên kết (link) hoặc tập tin đính kèm lạ, có dấu hiệu khả nghi. Cần lập tức chuyển các thư này đến địa chỉ tiepnhan@thuathienhue.gov.vn để bộ phận kỹ thuật hỗ trợ kiểm tra, ngăn chặn và xử lý, tránh phát tán thư điện tử có dấu hiệu khả nghi đến người sử dụng khác;

3. Kiểm tra, rà soát hệ thống thông tin đang sử dụng có khả năng bị ảnh hưởng bởi mã độc 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.

4. 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 Sở Thông tin và Truyền thông và các cơ quan chức năng về an toàn thông tin để phát hiện kịp thời các nguy cơ tấn công mạng;

5. Trong trường hợp cần thiết có thể liên hệ đầu mối hỗ trợ của Sở Thông tin và Truyền thông: Phòng Giám sát, điều hành an toàn, an ninh mạng - Trung tâm Giám sát, điều hành đô thị thông minh – Sở Thông tin và Truyền thông:

- *đ/c Hoàng Diên Kỷ; điện thoại: 0906 760 759;*

- *đ/c La Thức; điện thoại: 0772 428 218;*

Trân trọng./.

Nơi nhận:
- Như trên;
- UBND tỉnh (để bc);
- Cục ATTT (để bc);
- Công an tỉnh (để p/h);
- BGĐ Sở;
- P.CNTT, HueIOC;
- Lưu: VT.

GIÁM ĐỐC

Nguyễn Xuân Sơn

Phụ lục

THÔNG TIN CHI TIẾT VỀ MÃ ĐỘC

(Kèm theo Công văn số 1716 /STTTT-IOC ngày 18 /6/2024 của Sở Thông tin và Truyền thông tỉnh Thừa Thiên Huế)

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

Gần đây, đã phát hiện và ghi nhận các hành vi tấn công trái phép trên không gian mạng của nhóm tấn công Mustang Panda trong chiến dịch nhằm vào tổ chức tại Việt Nam. Chiến dịch tấn công lần này của nhóm Mustang Panda sử dụng các mồi nhử xoay quanh lĩnh vực giáo dục và thuế, áp dụng nhiều góc tiếp cận. Mục tiêu mà nhóm hướng tới là các tổ chức chính phủ, tổ chức phi lợi nhuận, tổ chức giáo dục,…

Hai chiến dịch tấn công được ghi nhận vào tháng 05 và tháng 04 năm 2024 nhằm tới Việt Nam đã sử dụng file văn bản có nội dung liên quan tới cơ quan thuế và tổ chức giáo dục. Cả hai chiến dịch đều có điểm chung là bắt nguồn từ các email lừa đảo có đính kèm file độc hại.

Chiến dịch có nhiều giai đoạn phức tạp, khai thác các công cụ như "forfiles.exe" để thực thi file HTA độc hại lưu trên máy chủ từ xa. Ngoài ra, Mustang Panda còn sử dụng PowerShell, VBScript và batch file trong chiến dịch. Để tránh bị phát hiện, nhóm đối tượng đã nhúng các file văn bản này vào các file .LNK độc hại. Chiến dịch sử dụng kỹ thuật DLL sideloading với rundll32 để thực thi DLL độc hại trên hệ thống.

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

Dưới đây là một số IoC được ghi nhận

47eb43acdd342d3975000f650cf656d9f0f759780d85f16d806d6b9a70f1be46	SHA256	LNK File
9375b508e981ed792742f1f3b831ea6647191c261e0d3cd61e60645251ba7df7	SHA256	LNK File
cd10f98c2dbcc0c8fe3f0ed19efb1b2340f67b1138a55b0bb8d1e3dfb985df51	SHA256	HPCustPartUI.dll

bce44453835ce96e49046ff618749a9533c290504c3d7559b3a63969b9f3ef13	SHA256	wwlib.dll
57ba7d5093ec54b0223e6a826f6cb5e019a353963ddbac8420036f7374b28f62	SHA256	Book.dll
96cf65bb1ac9735c6a1100944d0f46343bb74f3a3c05bc6282271184b872198e	SHA256	Vanban_8647.PDF_update.hta
fe721743a87c2f2767c031ccac337c1fb1ae5e92384738dd90c65d3b1617a341	SHA256	Vanban_8647.PDF.ps1
0ea669d3ef2ae00f25ccb4fef4805c6fd7f9816c37afb8957b3d4ace065e1d95	SHA256	tempdata.dat
4c805f281923ffc2214f4fe48f31ea392b13b710969a18ad6b6b561744cd3875	SHA256	init.txt
968b3de170038522deae02b9b96c45cfc6a5c70fa0ddfaf29320d0d0d36aabfa	SHA256	getdata.ps1
hxxp://mega.vlvlvlvl[.]site/Vanban_8647.PDF_update.hta	URL	Download URL
hxxp://mega.vlvlvlvl[.]site/HP.exe	URL	Download URL
hxxp://mega.vlvlvlvl[.]site/HPCustPartUI.dll	URL	Download URL
hxxp://mega.vlvlvlvl[.]site/Vanban_8647.PDF.ps1	URL	Download URL
hxxp://payment.tripadviso[.]online/tempdata.dat	URL	Download URL

hxxp://vibm[.]vn/init.txt	URL	Download URL
hxxp://megacybernews[.]com/newrun.ps1	URL	Download URL
hxxp://megacybernews[.]com/getdata.ps1	URL	Download URL
hxxp://megacybernews[.]com/stage2.2.ps1	URL	Download URL
hxxp://megacybernews[.]com/checkin.php	URL	Download URL
hxxp://megacybernews[.]com/book.dll	URL	Download URL
hxxp://megacybernews[.]com/unikey.exe	URL	Download URL
hxxp://megacybernews[.]com/wwlib.dll	URL	Download URL
mega.vlvlvlvl[.]site	Domain	C&C
payment.tripadviso[.]online	Domain	C&C
vibm[.]vn	Domain	C&C
megacybernews[.]com	Domain	C&C

2. Tài liệu tham khảo

https://cyble.com/blog/vietnamese-entities-targeted-by-china-linked-mustang-panda-in-cyber-espionage/