BỘ GIAO THÔNG VẬN TẢI
CỤC HÀNG HẢI VIỆT NAM

Số: 2860 /CHHVN-KHCNMT
V/v cảnh báo các lỗ hổng bảo mật tháng 6 năm 2024 (lần 2).

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

Hà Nội, ngày 28 tháng 6 năm 2024

Kính gửi:
- Các đơn vị trực thuộc.
- Công ty TNHH MTV Thông tin điện tử hàng hải Việt Nam.

Cục Hàng hải Việt Nam nhận được thông tin cảnh báo về nguy cơ tấn công mạng liên quan tới các lỗ hổng bảo mật trong các sản phẩm của Microsoft (*Message Queuing (MSMQ), Outlook, Windows Wi-Fi Driver, Office, SharePoint Server*) và cảnh báo nhóm APT "Mustang Panda" thực hiện chiến dịch tấn công nhằm vào Việt Nam.

Để bảo đảm an toàn thông tin, an ninh mạng cho Hệ thống công nghệ thông tin của Cục Hàng hải Việt Nam và các đơn vị trực thuộc, Cục Hàng hải Việt Nam yêu cầu Công ty TNHH MTV Thông tin điện tử hàng hải Việt Nam và các đơn vị trực thuộc chủ động thực hiện các biện pháp sau:

1. Kiểm tra, rà soát, xác định các hệ thống thông tin có khả năng bị ảnh hưởng bởi các mã độc và chiến dịch tấn công nêu trên. Chủ động theo dõi các thông tin liên quan đến mã độc từ đơn vị phát triển (*xây dựng*) phần mềm, sản xuất thiết bị phần cứng nhằm thực hiện nâng cấp lên phiên bản mới nhất để tránh nguy cơ bị tấn công; và theo dõi các thông tin liên quan đến các chiến dịch tấn công để ngăn chặn, xử lý kịp thời khi phát hiện các dấu hiệu bị tấn công. Danh sách các lỗ hổng bảo mật và thông tin chi tiết về chiến dịch tấn công tại Phụ lục gửi kèm theo.

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, an ninh mạng để phát hiện kịp thời các nguy cơ tấn công mạng. Trường hợp cần thiết, liên hệ với Trung tâm Công nghệ thông tin - Bộ Giao thông vận tải (*ông Dương Đình Trung - số điện thoại 0985366388*) và các cơ quan chức năng về an toàn, an ninh mạng để được hỗ trợ xử lý.

Cục Hàng hải Việt Nam yêu cầu các đơn vị triển khai thực hiện./.

Nơi nhận:
- Như trên;
- Cục trưởng (*để b/c*);
- Lưu: VT, KHCNMT.

KT. CỤC TRƯỞNG
PHÓ CỤC TRƯỞNG

BỘ GIAO THÔNG VẬN TẢI
CỤC HÀNG HẢI VIỆT NAM

Nguyễn Hoàng

Phụ lục 01

Thông tin về các lỗ hổng bảo mật trong sản phẩm Microsoft

1. Thông tin các lỗ hổng bảo mật

STT	CVE	Mô tả	Link tham khảo
1	CVE-2024-30080	- Điểm CVSS: 9.8 (Nghiêm trọng) - Mô tả: Lỗ hổng trong Microsoft Message Queuing (MSMQ) cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows 10, Windows 11, Windows Server 2008, 2012, 2016, 2019, 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30080
2	CVE-2024-30103	- Điểm CVSS: 8.8 (Cao) - Mô tả: Lỗ hổng trong Microsoft Outlook cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Outlook 2016, 2019, Microsoft 365 Apps for Enterprise, Microsoft Office LTSC 2021.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30103
3	CVE-2024-30078	- Điểm CVSS: 8.8 (Cao) - Mô tả: Lỗ hổng trong Windows Wi-Fi Driver cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Windows 10, Windows 11, Windows Server 2008, 2012, 2016, 2019, 2022.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30078
4	CVE-2024-30101 CVE-2024-30102 CVE-2024-30104	- Điểm CVSS: 7.8 (Cao) - Mô tả: Lỗ hổng trong Microsoft Office cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft Outlook 2016, 2019, Microsoft 365 Apps for Enterprise, Microsoft Office LTSC 2021.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30101 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30102 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30104

5	CVE-2024-30100	- Điểm CVSS: 7.8 (Cao) - Mô tả: Lỗ hổng trong Microsoft SharePoint Server cho phép đối tượng tấn công thực thi mã từ xa. - Ảnh hưởng: Microsoft SharePoint Server 2019, Microsoft SharePoint Enterprise Server 2016, Microsoft SharePoint Server Subscription Edition.	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30100

2. Hướng dẫn khắc phục

Biện pháp tốt nhất để khắc phục là cập nhật bản vá cho các lỗ hổng bảo mật nêu trên theo hướng dẫn của hãng. Các đơn vị tham khảo các bản cập nhật phù hợp cho các sản phẩm đang sử dụng tại link nguồn tham khảo của phụ lục.

3. Tài liệu tham khảo

https://msrc.microsoft.com/update-guide

https://www.zerodayinitiative.com/blog/2024/6/11/the-june-2024-security-update-review

Phụ lục 02

THÔNG TIN CHI TIẾT VỀ CHIẾN DỊCH TẤN CÔNG

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 5/2024 và tháng 4/2024 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

47eb43acdd342d3975000f650cf656d9f0f75 9780d85f16d806d6b9a70f1be46	SHA256	LNK File
9375b508e981ed792742f1f3b831ea664719 1c261e0d3cd61e60645251ba7df7	SHA256	LNK File
cd10f98c2dbcc0c8fe3f0ed19efb1b2340f67b 1138a55b0bb8d1e3dfb985df51	SHA256	HPCustPartUI.dll
bce44453835ce96e49046ff618749a9533c29 0504c3d7559b3a63969b9f3ef13	SHA256	wwlib.dll
57ba7d5093ec54b0223e6a826f6cb5e019a3 53963ddbac8420036f7374b28f62	SHA256	Book.dll
96cf65bb1ac9735c6a1100944d0f46343bb7 4f3a3c05bc6282271184b872198e	SHA256	Vanban_8647.PDF _update.hta
fe721743a87c2f2767c031ccac337c1fb1ae5e 92384738dd90c65d3b1617a341	SHA256	Vanban_8647.PDF.ps 1
0ea669d3ef2ae00f25ccb4fef4805c6fd7f981 6c37afb8957b3d4ace065e1d95	SHA256	tempdata.dat
4c805f281923ffc2214f4fe48f31ea392b13b7 10969a18ad6b6b561744cd3875	SHA256	init.txt
968b3de170038522deae02b9b96c45cfc6a5c 70fa0ddfaf29320d0d0d36aabfa	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/