Khuyến nghị về Mối Đe Dọa Mạng từ DPRK

Phát hành: **Ngày 15 tháng 4, 2020**

Chủ đề: **Hướng dẫn về Mối Đe Dọa Mạng từ Triều Tiên**

Bộ Ngoại Giao, Bộ Tài Chính, Bộ An Ninh Nội Địa và Cục Điều tra Liên Bang Hoa Kỳ đưa ra văn bản khuyến nghị này như một tài liệu đầy đủ về mối đe dọa của Triều Tiên đối với cộng đồng quốc tế, lực lượng bảo vệ hệ thống mạng và công chúng. Khuyến nghị này nhấn mạnh mối đe dọa không gian mạng gây ra do Triều Tiên – tên chính thức là Cộng Hòa Dân Chủ Nhân Dân Triều Tiên (DPRK) - và đưa ra các bước đề nghị nhằm giảm thiểu mối đe dọa này. Cụ thể, Phụ Lục 1 liệt kê các nguồn trợ giúp của chính phủ Hoa Kỳ liên quan đến mối đe dọa từ DPRK và Phụ Lục 2 có đường liên kết vào các bản báo cáo của Hội đồng Chuyên gia - Ủy ban Trừng Phạt DPRK chiếu Nghị quyết 1718 của Liên Hợp Quốc.

Các hoạt động không gian mạng độc hại của DPRK đe dọa Hoa Kỳ và rộng hơn là cộng đồng quốc tế, đặc biệt đe dọa đáng kể đến tính toàn vẹn và ổn định của hệ thống tài chính quốc tế. Dưới áp lực của các trừng phạt mạnh mẽ của Hoa Kỳ và Liên Hợp Quốc, DPRK đã ngày càng dựa vào các hoạt động bất hợp pháp - bao gồm cả tội phạm trên mạng - để mang lại thu nhập cho các chương trình vũ khí hủy diệt hàng loạt và tên lửa đạn đạo. Đặc biệt, Hoa Kỳ rất quan ngại về các hoạt động mạng độc hại của Triều Tiên, mà chính phủ Hoa Kỳ gọi là HIDDEN COBRA (HỔ MANG ẨN). DPRK có khả năng tiến hành các hoạt động mạng gây rối hoặc phá hoại, ảnh hưởng đến cơ sở hạ tầng quan trọng của Hoa Kỳ. DPRK cũng dùng các khả năng mạng để đánh cắp từ các tổ chức tài chính, và đã biểu lộ một mô hình hoạt động mạng gây rối và phá hoại, hoàn toàn không phù hợp với sự nhất trí ngày càng tăng của quốc tế về những gì cấu thành hành vi có trách nhiệm của Nhà nước trong không gian mạng.

Hoa Kỳ hợp tác chặt chẽ với các quốc gia đồng quan điểm, dồn nỗ lực và lên án các hành vi gây rối, phá hoại, hoặc hành vi gây bất ổn trong không gian mạng. Ví dụ, vào tháng 12, 2017; Úc, Canada, New Zealand, Hoa Kỳ và Vương quốc Anh đã công khai quy kết vụ tấn công mã độc tống tiền WannaCry 2.0 là do DPRK và các nước này đã tố cáo hoạt động mạng độc hại và vô trách nhiệm của DPRK. Đan Mạch và Nhật cũng đã đưa ra tuyên bố ủng hộ lời tố cáo chung về vụ tấn công mã độc tống tiền WannaCry 2.0, đã ảnh hưởng đến hàng trăm ngàn máy tính trên toàn thế giới vào tháng 5, 2017.

Điều quan trọng là cộng đồng quốc tế, lực lượng bảo vệ hệ thống mạng, và công chúng phải luôn cảnh giác và cùng nhau hợp tác để giảm thiểu mối đe dọa mạng do Triều Tiên gây ra.

Các hoạt động mạng độc hại của DPRK nhắm vào Lĩnh vực Tài Chính

Rất nhiều thực thể đã được Liên Hợp Quốc và Hoa Kỳ chỉ định là tác nhân không gian mạng của DPRK, chẳng hạn như Tổng Cục Trinh Sát. Các tác nhân không gian mạng do chính phủ DPRK bảo trợ hầu hết bao gồm tin tặc, chuyên viên mã hóa và các nhà thiết kế phần mềm; họ thực hiện các hoạt động gián điệp, kích hoạt mạng để đánh cắp, nhắm vào các tổ chức tài chính và các hình thức trao đổi tiền kỹ thuật số, cùng các hoạt động mang động cơ chính trị chống lại các công ty truyền thông nước ngoài. Họ gầy dựng và triển khai hàng loạt công cụ phần mềm độc hại trên toàn thế giới tạo điều kiện cho các hoạt động này và ngày càng phát triển tinh vi. Các thủ đoạn thường dùng để tạo lợi nhuận bất hợp pháp do các tác nhân mạng được chính phủ DPRK bảo trợ bao gồm, nhưng không chỉ giới hạn các hình thức sau:

Trộm cắp Tài Chính trên Mạng và Rửa Tiền. Báo cáo giữa kỳ năm 2019 của Hội đồng Chuyên gia chiếu Nghị quyết 1718 của Hội Đồng Bảo An LHQ (gọi tắt là Báo cáo giữa kỳ 2019 của POE) tuyên bố rằng DPRK ngày càng gia tăng khả năng tạo ra thu nhập, bất chấp những trừng phạt của Hội Đồng Bảo An LHQ, thông qua việc sử dụng các hoạt động mạng độc hại để đánh cắp từ các tổ chức tài chính với các công cụ và thủ đoạn ngày càng tinh vi. Báo cáo giữa kỳ 2019 của POE cũng lưu ý rằng, trong một số trường hợp, các hoạt động mạng độc hại này cũng đã nới rộng sang việc rửa tiền, thông qua nhiều thẩm quyền tài phán khác nhau. Báo cáo giữa kỳ 2019 của POE cũng đề cập rằng, qua công tác điều tra hàng chục vụ trộm bị tình nghi là do DPRK kích hoạt mạng, họ đã thấy, tính đến thời điểm cuối năm 2019, DPRK đã mưu toan đánh cắp gần 2 tỷ đô la thông qua các hoạt động bất hợp pháp này. Các cáo buộc trong khiếu nại để đòi tịch thu của Bộ Tư Pháp vào tháng 3, 2020 nhất quán với nhiều phần trong kết luận của Hội đồng Chuyên gia (POE). Cụ thể, khiếu nại này trình bày những cách mà các tác nhân mạng Triều Tiên đã sử dụng cơ sở hạ tầng của Triều Tiên để thực hiện âm mưu xâm nhập vào các sàn trao đổi tiền kỹ thuật số, đánh cắp cả trăm triệu đô la tiền kỹ thuật số và rửa số tiền trên.

Chiến Dịch Tống Tiền. Các tác nhân mạng DPRK cũng đã tiến hành các chiến dịch tống tiền vào các thực thể của các nước thứ ba, bằng cách chiếm quyền kiểm soát mạng của một thực thể và đe dọa sẽ đánh sập nếu thực thể đó không trả một số tiền chuộc. Trong một số trường hợp, các tác nhân mạng DPRK cũng đã yêu cầu các nạn nhân thanh toán theo dạng ngụy trang là các thỏa thuận trả tiền tư vấn dài hạn để đảm bảo rằng sẽ không có bất cứ hoạt động mạng độc hại nào sẽ xảy ra trong tương lai. Các tác nhân mạng DPRK cũng đươc thân chủ là bên thứ trả tiền để xâm nhập vào các trang web và tống tiền các mục tiêu mà thân chủ yêu cầu.

Cryptojacking/Đánh cắp mã. Báo cáo giữa kỳ 2019 của POE cũng cho biết POE đang điều tra việc DPRK sử dụng "cryptojacking" (đánh cắp mã), một âm mưu nhằm kiểm soát máy tính của nạn nhân và đánh cắp các tài nguyên của máy để khai thác tiền kỹ thuật số. POE cũng đã xác định được trong một vài sự cố, các máy tính bị nhiễm phần mềm cryptojacking độc hại đã chuyển những tài sản bị khai thác - phần lớn là tiền kỹ thuật số được nâng cấp thành tiền ẩn danh (đôi khi còn đươc gọi là đồng xu riêng tư – privacy coins) - đến các máy chủ được đặt tại DPRK, bao gồm cả tại trường Đại Học Kim Il Sung ở Bình Nhưỡng.

Các hoạt động này nêu bật việc DPRK sử dụng các phương tiện do mạng hỗ trợ để tạo thu nhập, đồng thời làm giảm tác động của lệnh trừng phạt và cho thấy rằng bất cứ quốc gia nào cũng có thể bị DPRK xen vào và khai thác. Cũng theo báo cáo giữa kỳ 2019 của POE, POE đang điều tra các hoạt động như vậy, và xem đó là mưu toan vi phạm các lệnh trừng phạt của LHQ đối với DPRK.

Các Hoạt Động Mạng mà Chính Phủ Hoa Kỳ Quy kết Công khai là do DPRK

DPRK đã nhiều lần nhắm vào các hệ thống mạng của chính phủ và quân đội Hoa Kỳ và các nước khác, cũng như các hệ thống mạng liên quan đến các thực thể tư nhân và hạ tầng cơ sở quan trọng, đánh cắp dữ liệu và thực hiện các hoạt động mạng gây rối và phá hoại. Đến nay, chính phủ Hoa Kỳ đã chính thức quy kết các sự cố mạng dưới đây là do các tác nhân mạng được chính phủ DPRK bảo trợ cùng các đồng phạm thực hiện:

- ***Sony Pictures***. Vào tháng 11, 2014, các tác nhân mạng do chính phủ DPRK bảo trợ bị cáo buộc đã tiến hành một cuộc tấn công mạng vào công ty Sony Pictures Entertainment (SPE) nhằm trả đũa cho bộ phim năm 2014 "The Interview". Các tác nhân mạng DPRK đột nhập vào hệ thống mạng của SPE, đánh cắp dữ liệu mật, đe dọa các giám đốc và nhân viên của SPE, và phá hoại cả ngàn máy tính.

    - Cập nhật cuộc Điều tra về Sony của FBI (19 tháng 12, 2014) https://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation
    - Khiếu nại Hình Sự của Bộ Tư Pháp về một lập trình viên do chế độ Triều Tiên hậu thuẫn (6 tháng 9, 2018) https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and

- ***Vụ Cướp Ngân Hàng Bangladesh***. Vào tháng 2, 2016, các tác nhân mạng do chính phủ DPRK bảo trợ cố gắng đánh cắp ít nhất 1 tỷ đô la từ các tổ chức tài chính trên toàn thế giới và bị cáo buộc đã đánh cắp 81 triệu từ Ngân Hàng Bangladesh qua các giao dịch trái phép trên hệ thống mạng Hiệp Hội Tài Chính Viễn Thông Liên Ngân Hàng Toàn Cầu (SWIFT). Theo đơn khiếu nại, các tác nhân mạng DPRK đã truy cập vào các thiết bị đầu cuối của Ngân Hàng Bangladesh có tương tác với hệ thống mạng SWIFT, sau khi đã kiểm soát được hệ thống máy tính của ngân hàng qua các email lừa đảo mà chúng đã gửi cho các nhân viên ngân hàng này. Các tác nhân mạng của DPRK sau đó đưa ra các thông điệp giả mạo, có chứng thực của SWIFT, ra lệnh cho Ngân Hàng Dự Trữ Liên Bang New York chuyển tiền ra khỏi tài khoản của Ngân Hàng Bangladesh tại Ngân Hàng Dự Trữ Liên Bang để ký thác vào các tài khoản do những tác nhân mạng của DPRK kiểm soát.

    - Khiếu nại Hình Sự của Bộ Tư Pháp về một lập trình viên do chế độ Triều Tiên hậu thuẫn (6 tháng 9, 2018) https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and

- ***WannaCry 2.0***. Các tác nhân mạng do chính phủ DPRK bảo trợ đã soạn ra phần mềm tống tiền ransomware được gọi là WannaCry 2.0, cũng như hai phiên bản trước của

ransomware. Vào tháng 5, 2017, WannaCry 2.0 đã lây nhiễm hàng trăm ngàn máy tính tại các bệnh viện, trường học, doanh nghiệp, và tư gia trên hơn 150 quốc gia. Phần mềm WannaCry 2.0 mã hóa dữ liệu của máy bị nhiễm và tạo điều kiện để các tác nhân mạng đòi tiền chuộc, được thanh toán bằng tiền kỹ thuật số Bitcoin. Bộ Tài Chính đã chỉ định một lập trình viên người Triều Tiên đã tham gia trong âm mưu WannaCry 2.0, cũng như vai trò của anh ta trong cuộc tấn công mạng tại Sony Pictures và vụ cướp Ngân Hàng Bangladesh, đồng thời bộ này cũng chỉ định tổ chức mà anh ta làm việc là tác nhân mạng do DPRK bảo trợ.

- Cảnh báo Kỹ Thuật của CISA: Các Dấu hiệu liên quan đến Phần mềm Tống Tiền WannaCry (12 tháng 5, 2017) https://www.us-cert.gov/ncas/alerts/TA17-132A
- Họp Báo của Nhà Trắng để Quy Kết Phần mềm Tống Tiền WannaCry (19 tháng 12, 2017) https://www.whitehouse.gov/briefings-statements/press-briefing-on-the-attribution-of-the-wannacry-malware-attack-to-north-korea-121917/
- Khiếu nại Hình Sự của Bộ Tư Pháp về một lập trình viên do chế độ Triều Tiên hậu thuẫn (6 tháng 9, 2018) https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and
- Bộ Tài Chính nhắm Triều Tiên là thủ phạm nhiều cuộc tấn công mạng (6 tháng 9, 2018) https://home.treasury.gov/news/press-releases/sm473

- ***Chiến dịch FASTCash/Tiền mặt Nhanh.*** Từ cuối năm 2016, các tác nhân mạng do chính phủ DPRK bảo trợ tiến hành một kế hoạch rút tiền mặt gian lận, còn đươc gọi là "FASTCash" (Tiền Mặt Nhanh) để lấy căp hàng chục triệu đô la từ các máy ATM ở Châu Á và Châu Phi. Kế hoạch FASTCash đã kiểm soát từ xa các ứng dụng chuyển đổi thanh toán của máy chủ trong các ngân hàng để tạo điều kiện thuận lợi cho các giao dịch gian lận. Trong một vụ vào năm 2017, các tác nhân mạng DPRK đã tạo điều kiện để cùng một lúc rút được tiền mặt của các máy ATM ở hơn 30 quốc gia khác nhau. Trong một vụ khác vào năm 2018, các tác nhân mạng DPRK đã tạo điều kiện để cùng một lúc rút được tiền mặt của các máy ATM ở 23 quốc gia khác nhau.

  - Cảnh báo của CISA về Chiến dịch FASTCash (2 tháng10, 2018) https://www.us-cert.gov/ncas/alerts/TA18-275A
  - Báo cáo của CISA về Phân tích Phần mềm Độc hại: Phần mềm Độc hại Liên quan đến FASTCash (2 tháng 10, 2018) https://www.us-cert.gov/ncas/analysis-reports/AR18-275A

- ***Đột nhập vào Sàn Giao dịch Tiền Kỹ Thuật Số***. Như các chi tiết cáo buộc được nêu trong một khiếu nại của Bộ Tư Pháp vào tháng 4 năm 2018 để tịch thu tài sản đến từ nguồn gốc phi pháp, các tác nhân mạng do nhà nước DPRK bảo trợ đã đột nhập vào một sàn giao dịch tiền kỹ thuật số và đánh cắp gần 250 triệu đô la tiền kỹ thuật số. Khiếu nại mô tả thêm về cách các tài sản bị đánh cắp đã được rửa qua hàng trăm giao dịch tiền kỹ thuật số tự động, để che dấu nguồn gốc của các khoản tiền, nhằm ngăn cản lực lượng chấp pháp truy tìm tài sản. Khiếu nại cũng cho biết hai công dân Trung Quốc sau đó bị cáo buộc đã rửa tài sản thay mặt cho nhóm người Triều Tiên, nhận khoảng 91 triệu đô la từ các tài khoản do DPRK kiểm soát, cũng như thêm 9,5 triệu đô la từ vụ đột nhập vào một sàn giao dịch khác. Vào tháng 3 năm 2020, Bộ Tài

Chính đã chỉ định hai cá nhân này thuộc phạm vi trừng phạt về mạng và về DPRK, song hành với công bố của Bộ Tư Pháp rằng các cá nhân này trước đây đã bị truy tố về tội rửa tiền và chuyển tiền trái phép, và họ có 113 tài khoản tiền kỹ thuật số thuộc diện bị tịch thu.

- Các Trừng Phạt của Bộ Tài Chính đối với các Cá Nhân Rửa Tiền Mã Hóa cho Nhóm Lazarus (2 tháng 3, 2020) https://home.treasury.gov/news/press-releases/sm924
- Cáo trạng của Bộ Tư Pháp Buộc Tội Hai Công Dân Trung Quốc Rửa Tiền Mã Hóa do Đột Nhập vào Sàn Giao Dịch và Khiếu Nại Tịch Thu Dân Sự (2 tháng 3, 2020) https://www.justice.gov/opa/pr/two-chinese-nationals-charged-laundering-over-100-million-cryptocurrency-exchange-hack

Các Biện Pháp Chống Lại mối Đe dọa Mạng của DPRK

Triều Tiên nhắm vào các cơ sở hạ tầng trên toàn cầu nào được kích hoạt bằng mạng để tạo thu nhập cho các mục tiêu ưu tiên của thể chế, bao gồm các chương trình vũ khí hủy diệt hàng loạt. Chúng tôi rất mong các chính phủ, ngành công nghiệp, xã hội dân sự và mọi người thực hiện mọi hành động liên quan dưới đây để bảo vệ chính mình và chống lại mối đe dọa mạng DPRK:

- **Nâng cao Nhận thức về mối Đe dọa Mạng DPRK.** Nhấn mạnh tầm nguy hiểm, phạm vi và nhiều hoạt động mạng độc hại do DPRK thực hiện sẽ giúp nâng cao nhận thức chung trong cả lĩnh vực công và tư về mối đe dọa; tăng cường áp dụng và thực hiện các biện pháp phòng ngừa và giảm thiểu rủi ro một cách thích hợp.

- **Chia sẻ Thông tin Kỹ thuật về mối Đe dọa Mạng DPRK**. Chia sẻ thông tin ở cả cấp quốc gia lẫn quốc tế để phát hiện và phòng thủ chống lại mối đe dọa không gian mạng từ DPRK sẽ tạo điều kiện để củng cố an ninh mạng của các mạng và hệ thống. Phương thức thực hành tốt nhất nên được chia sẻ giữa chính phủ và khu vực tư nhân. Theo các điều khoản của Đạo luật Chia sẻ Thông tin An ninh mạng năm 2015 (Luật Hoa Kỳ Phần 6, các đoạn 1501-1510), các thực thể không thuộc về liên bang có thể chia sẻ các dấu hiệu đe dọa không gian mạng và các biện pháp phòng thủ liên quan đến HIDDEN COBRA (HỔ MANG ẨN) với các thực thể liên bang và không thuộc liên bang.

- **Thực hiện và Thúc đẩy các cách Thực hành An ninh Mạng Tốt nhất**. Áp dụng các biện pháp – cả về kỹ thuật và hành vi ứng xử – để tăng cường an ninh mạng sẽ tạo điều kiện cho cơ sở hạ tầng mạng của cả Hoa Kỳ và toàn cầu trở nên an toàn và linh hoạt hơn. Các tổ chức tài chính, bao gồm các doanh nghiệp có dịch vụ tiền tệ, nên thực hiện các bước độc lập để chống lại các hoạt động mạng DPRK độc hại. Các bước này có thể bao gồm, nhưng không chỉ giới hạn vào, việc chia sẻ thông tin về mối đe dọa thông qua các kênh của chính phủ và/hoặc ngành, phân đoạn mạng để giảm thiểu rủi ro, duy trì thường xuyên các bản sao dữ liệu để dự phòng, tiến hành đào tạo nâng cao nhận thức về các thủ đoạn gian trá xã hội thông thường, thực hiện các chính sách quản lý việc chia sẻ thông tin và truy cập mạng, và thành lập các kế hoạch ứng phó sự cố mạng. Mô hình Trưởng thành Khả năng Bảo mật Không gian Mạng của Bộ Năng Lượng (C2M2) và Khung An ninh Mạng của Viện Tiêu chuẩn và Công nghệ Quốc gia (NIST Cybersecutity Framework)

cung cấp hướng dẫn về việc thiết lập và thực hiện các cách thực hành an ninh mạng vững chắc. Như Cục An ninh Cơ sở Hạ tầng và An ninh Mạng (CISA) trình bày, Phụ lục I cung cấp nhiều nguồn lực, bao gồm các cảnh báo kỹ thuật và báo cáo phân tích phần mềm độc hại, tạo điều kiện để các nhà bảo vệ mạng xác định và giảm tiếp xúc với các hoạt động mạng độc hại.

- **Thông báo cho lực lượng Chấp Pháp.** Nếu một tổ chức nghi ngờ rằng họ là nạn nhân của hoạt động mạng độc hại, phát sinh từ DPRK hay nơi nào khác, việc thông báo cho cơ quan thực thi pháp luật một cách kịp thời là rất quan trọng. Điều này không những đẩy nhanh quy trình điều tra, mà trong trường hợp phạm tội tài chính, có thể làm tăng cơ hội thu hồi tài sản bị đánh cắp.

  Cơ quan thực thi pháp luật của Hoa Kỳ đã tịch thu hàng triệu đô la tiền kỹ thuật số do các tác nhân Triều Tiên đánh cắp. Tất cả các thể loại tổ chức tài chính, bao gồm các doanh nghiệp có dịch vụ tiền bạc, một mặt được khuyến khích hợp tác bằng cách tuân thủ các yêu cầu thực thi pháp luật của Hoa Kỳ về cung cấp thông tin liên quan đến các mối đe dọa mạng, và một mặt bằng cách chỉ rõ các tài sản có thể bị tịch thu ngay khi nhận được yêu cầu của cơ quan chấp pháp Hoa Kỳ hoặc theo lệnh của tòa án Hoa Kỳ, và bằng cách hợp tác với cơ quan chấp pháp Hoa Kỳ để hỗ trợ việc tịch thu các tài sản đó.

- **Tăng cường Chống Rửa Tiền (AML) / Chống Tài Trợ Khủng Bố (CFT) / Tuân thủ chính sách Chống Phổ Biến Hoạt Động Tài Chính Trái Phép (CPF).** Các quốc gia nên thực hiện nhanh chóng và hiệu quả các tiêu chuẩn của Lực lượng Đặc nhiệm Tài chính (FATF) về AML/CFT/CPF. Điều này bao gồm việc đảm bảo rằng các tổ chức tài chính và các đơn vị có liên quan đến tiêu chuẩn này đều áp dụng các biện pháp giảm thiểu rủi ro ăn khớp với các tiêu chuẩn, các tuyên bố và hướng dẫn công khai của FATF. Cụ thể, FATF đã kêu gọi tất cả các quốc gia áp dụng các biện pháp đối phó để bảo vệ hệ thống tài chính quốc tế trước các hoạt động rửa tiền, các hoạt động tài trợ khủng bố và các rủi ro phổ biến hoạt động tài chính trái phép phát sinh từ DPRK đang diễn ra[1]. Điều này bao gồm khuyến cáo tất cả các tổ chức tài chính và các đơn vị có liên quan đến tiêu chuẩn này phải chú ý đặc biệt đến các mối quan hệ kinh doanh và giao dịch với DPRK, bao gồm các công ty, tổ chức tài chính của DPRK và những người thay mặt họ. Để phù hợp với Nghị quyết 2270 của Hội đồng Bảo an Liên Hợp Quốc, Đoạn thực hành 33, các Quốc gia Thành viên nên đóng cửa các chi nhánh, công ty con và văn phòng đại diện của các ngân hàng DPRK bên trong lãnh thổ của mình và chấm dứt mối quan hệ tương ứng với các ngân hàng DPRK.

  Hơn nữa, vào tháng 6, 2019, FATF đã sửa đổi các tiêu chuẩn để yêu cầu tất cả các quốc gia điều tiết và giám sát các nhà cung cấp dịch vụ tài sản kỹ thuật số, bao gồm các sàn trao đổi tiền kỹ thuật số, nhằm giảm thiểu rủi ro khi giao dịch tiền kỹ thuật số. Các nhà cung cấp dịch vụ tài sản kỹ thuật số nên cảnh giác với những thay đổi trong hoạt động của khách hàng, vì hoạt động kinh doanh của họ có thể bị lợi dụng để tạo điều kiện cho hoạt động rửa tiền, tài trợ khủng bố và phổ biến hoạt động tài chính trái phép. Hoa Kỳ đặc biệt quan tâm đến các sàn cung cấp chức năng thanh toán ẩn danh và dịch vụ tài

[1] *Có thể xem đầy đủ Lời Kêu gọi Hành động của FATF về Triều Tiên tại đây:* https://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/documents/call-for-action-february-2020.html

khoản mà không có giám sát giao dịch, không báo cáo hoạt động đáng ngờ và khách hàng không theo đúng quy trình, ngoài các nghĩa vụ khác.

Các tổ chức tài chính của Hoa Kỳ, bao gồm các nhà cung cấp dịch vụ tài sản kỹ thuật số có trụ sở ở nước ngoài, thực hiện kinh doanh toàn bộ hoặc phần lớn ở Hoa Kỳ, các doanh nghiệp và cá nhân có liên quan đến tiêu chuẩn này phải đảm bảo rằng họ tuân thủ các nghĩa vụ pháp lý của mình thể theo Đạo luật Bảo mật Ngân hàng (được thực hiện thông qua các quy định của Mạng lưới Thi Hành Tội phạm Tài chính (FinCEN) thuộc Bộ Tài Chính, có ghi trong Công Báo 31 CFR, Chương X). Đối với các tổ chức tài chính, các nghĩa vụ này bao gồm việc thiết lập và duy trì các chương trình chống rửa tiền hiệu quả, được thiết kế một cách hợp lý nhằm ngăn chặn các cơ sở kinh doanh dịch vụ tiền tệ bị lợi dụng cho các hoạt động rửa tiền và tài trợ cho các hoạt động khủng bố, đồng thời xác định và báo cáo các giao dịch đáng ngờ, gồm cả những đối tượng đã thực hiện, bị ảnh hưởng hoặc tạo điều kiện cho các sự kiện diễn tiến qua mạng hoặc tài chính bất hợp pháp liên quan đến tài sản kỹ thuật số, khi báo cáo các hoạt động đáng ngờ cho FinCEN.

Hợp tác quốc tế. Để chống lại các hoạt động mạng độc hại của DPRK, Hoa Kỳ thường xuyên giao thiệp với các quốc gia trên thế giới để nâng cao nhận thức về mối đe dọa không gian mạng từ DPRK bằng cách chia sẻ thông tin và tang chứng thông qua ngoại giao, quân sự, chấp pháp và tư pháp, bảo vệ mạng và các kênh khác. Để cản trở những nỗ lực của DPRK nhằm đánh cắp tiền tệ thông qua các phương tiện không gian mạng và bảo vệ chống lại các hoạt động mạng độc hại của DPRK, Hoa Kỳ mạnh mẽ khuyến khích các quốc gia tăng cường phòng thủ mạng, đóng cửa liên doanh DPRK ở các nước thứ ba và trục xuất nhân viên công nghệ thông tin (IT) của Triều Tiên làm việc ở nước ngoài theo cách phù hợp với luật pháp quốc tế hiện hành. Nghị quyết của Hội đồng Bảo an Liên Hợp Quốc năm 2017 yêu cầu tất cả các Quốc gia Thành viên phải hồi hương công dân DPRK có thu nhập ở nước ngoài, bao gồm cả nhân viên IT, không quá ngày 22 tháng 12 năm 2019. Hoa Kỳ cũng tìm cách nâng cao năng lực của chính phủ và tư nhân nước ngoài để hiểu, xác định, chống lại, điều tra, truy tố và ứng phó với các mối đe dọa trên mạng của DPRK và tham gia các nỗ lực quốc tế nhằm đảm bảo sự ổn định của không gian mạng

<u>Hậu quả của việc tham gia vào các hành vi bị nghiêm cấm hoặc bị trừng phạt</u>

Các cá nhân và tổ chức tham gia hoặc hỗ trợ hoạt động liên quan đến mạng của DPRK, bao gồm việc xử lý các giao dịch tài chính liên quan, nên ý thức về những hậu quả tiềm ẩn của việc tham gia vào các hành vi bị cấm hoặc bị trừng phạt.

Văn phòng Kiểm soát Tài sản Nước ngoài của Bộ Tài Chính (OFAC) có thẩm quyền áp dụng các biện pháp trừng phạt đối với bất kỳ người nào được xác định là có, trong số những điều khác:

- Tham gia các hoạt động đáng kể để làm suy yếu an ninh mạng, thay mặt cho Chính phủ Triều Tiên hoặc Đảng Lao động Triều Tiên;
- Hoạt động trong ngành công nghệ thông tin (IT) tại Triều Tiên;
- Tham gia vào các hoạt động mạng độc hại khác; hoặc
- Tham gia ít nhất một lần xuất nhập đáng kể từ Triều Tiên bất kỳ hàng hóa, dịch vụ hoặc công nghệ nào.

Ngoài ra, nếu Bộ trưởng Tài chính, tham khảo ý kiến của Bộ trưởng Ngoại giao, xác định rằng một tổ chức tài chính nước ngoài đã cố tình thực hiện hoặc tạo điều kiện giao dịch quan trọng với Triều Tiên, hoặc cố tình thực hiện hoặc tạo điều kiện cho một giao dịch quan trọng thay mặt cho một người đã bị chỉ định theo Sắc lệnh Hành pháp Liên quan đến Triều Tiên, hoặc theo Sắc lệnh Hành pháp 13382 (Những người thực hiện và Những người trợ giúp vi phạm luật cấm Vũ khí Hủy diệt Hàng loạt) đối với các hoạt động liên quan đến Triều Tiên, tổ chức này có thể bị, ngoài các khả năng cấm đoán khác, mất khả năng duy trì một tài khoản chi trả hoặc ký thác tại Hoa Kỳ.

OFAC sẽ điều tra các hành vi rõ ràng vi phạm các quy định về trừng phạt và thực thi thẩm quyền chấp pháp, như đã nêu trong Hướng dẫn Thực thi Trừng phạt Kinh tế, có ghi trong Công Báo 31 CFR phần 501, phụ lục A. Người vi phạm Quy định Trừng phạt Triều Tiên, có ghi trong Công Báo 31 CFR phần 510, có thể bị phạt tiền về mặt dân sự ở mức tối đa theo luật hiện hành hoặc gấp đôi giá trị của giao dịch đang bị xử lý.

Báo cáo giữa kỳ 2019 của POE có lưu ý việc DPRK sử dụng, và mưu toan sử dụng các phương tiện hỗ trợ mạng để đánh cắp tiền từ các ngân hàng và các sàn trao đổi tiền kỹ thuật số có thể là hành động vi phạm nhiều Nghị quyết của Hội đồng Bảo an Liên Hợp Quốc (UNSCR) (ví dụ, Đoạn thực hành (OP) số 8(d) của UNSCR 1718; các OP số 8 và 11 của UNSCR 2094; và OP số 32 của UNSCR 2270). Các UNSCR khác liên quan đến DPRK cũng cung cấp các cơ chế khác nhau để khuyến khích tuân thủ các biện pháp trừng phạt liên quan đến DPRK do Liên Hợp Quốc áp đặt. Ví dụ, Ủy ban 1718 của Hội đồng Bảo an Liên Hợp Quốc có thể áp dụng các biện pháp trừng phạt có mục tiêu (ví dụ đóng băng tài sản và cấm du hành đối với cá nhân) đối với bất kỳ cá nhân hoặc tổ chức nào tham gia giao dịch kinh doanh với các thực thể mà Liên Hợp Quốc đã chỉ định hoặc trốn tránh trừng phạt.

Bộ Tư Pháp truy tố hình sự các hành vi cố ý vi phạm luật trừng phạt hiện hành, như Đạo luật Quyền lực Kinh tế Khẩn cấp Quốc tế, Luật Hoa Kỳ Phần 50 Đoạn 1701 và kế tiếp. Những người cố tình vi phạm các luật đó có thể phải đối mặt với án tù lên tới 20 năm, số tiền phạt lên tới 1 triệu đô la hoặc gấp đôi số lợi nhuận gộp, tùy theo số nào lớn hơn; và bị tịch thu tất cả các khoản tiền liên quan đến các giao dịch đó. Bộ Tư Pháp cũng truy tố hình sự các hành vi cố ý vi phạm Đạo luật Bảo mật Ngân hàng (BSA), Luật Hoa Kỳ Phần 31 các Đoạn 5318 và 5322, trong đó yêu cầu các tổ chức tài chính, ngoài các điều khác, phải duy trì các chương trình chống rửa tiền hiệu quả và nộp các báo cáo nhất định đến FinCEN. Những người vi phạm BSA có thể bị phạt tù tới 5 năm, phạt tiền lên tới 250.000 đô la, và có khả năng bị tịch thu tài sản liên quan đến các vi phạm. Nếu hợp lý, Bộ Tư Pháp cũng sẽ truy tố hình sự các tập đoàn và các thực thể khác vi phạm các đạo luật này. Bộ Tư Pháp cũng làm việc với các đối tác nước ngoài để chia sẻ bằng chứng hỗ trợ cho các cuộc điều tra và truy tố hình sự của nhau.

Theo Luật Hoa Kỳ Phần 31 Đoạn 5318(k), Bộ trưởng Tài chính hoặc Bộ trưởng Tư pháp có thể tống đạt trát yêu cầu một tổ chức tài chính nước ngoài có tài khoản ngân hàng tương ứng tại Hoa Kỳ xuất trình hồ sơ mà tổ chức này đang lưu ở nước ngoài. Khi Bộ trưởng Tài chính hoặc Bộ trưởng Tư pháp thông báo bằng văn bản cho tổ chức tài chính Hoa Kỳ rằng một tổ chức tài chính nước ngoài đã không tuân thủ trát yêu cầu đó, tổ chức tài chính Hoa Kỳ phải chấm dứt quan hệ giao dịch ngân hàng với tổ chức tài chính nước ngoài đó trong vòng mười ngày làm việc. Không thực hiện điều này có thể dẫn đến việc các tổ chức tài chính Hoa Kỳ sẽ bị phạt dân sự mỗi ngày.

Chương trình Tiền thưởng cho Công lý khi cung cấp thông tin về DPRK

Nếu bạn có thông tin về các hoạt động bất hợp pháp trong không gian mạng của DPRK, bao gồm các hoạt động trong quá khứ hoặc đang diễn ra, và cung cấp thông tin đó qua chương trình Tiền thưởng cho Công lý của Bộ Ngoại giao, bạn có thể nhận tiền thưởng lên tới 5 triệu đô la. Để biết thêm chi tiết, vui lòng truy cập www.rewardsforjustice.net.

PHỤ LỤC I: Thông tin Công cộng của Chính phủ Hoa Kỳ và các Nguồn Hỗ trợ Chống lại Đe dọa Mạng từ DPRK

Văn phòng Giám đốc Tình báo Quốc gia về Đánh giá các mối Đe dọa Hàng năm trên toàn Thế giới của Cộng Đồng Tình báo Hoa Kỳ. Năm 2019, Cộng đồng Tình báo Hoa Kỳ đã đánh giá rằng DPRK gây ra mối đe dọa mạng đáng kể cho các tổ chức tài chính, vẫn là mối đe dọa gián điệp trên mạng và duy trì được khả năng thực hiện các cuộc tấn công mạng gây rối. DPRK tiếp tục sử dụng các khả năng không gian mạng để đánh cắp từ các tổ chức tài chính nhằm mang lại thu nhập. Các hoạt động tội phạm mạng của Bình Nhưỡng bao gồm các nỗ lực đánh cắp hơn 1,1 tỷ đô la từ các tổ chức tài chính trên toàn thế giới – bao gồm một vụ đánh cắp trót lọt trên mạng với số tiền cướp được ước tính đến 81 triệu đô la của Ngân hàng Bangladesh. Báo cáo có thể xem tại https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf.

Báo cáo Kỹ thuật của Cơ quan An ninh Cơ Sở Hạ Tầng và An Ninh Mạng (CISA). Chính phủ Hoa Kỳ đề cập đến các hoạt động không gian mạng độc hại của DPRK với tên HIDDEN COBRA (HỔ MANG ẨN). Báo cáo HIDDEN COBRA cung cấp các chi tiết về kỹ thuật của các công cụ và cơ sở hạ tầng mà các tác nhân không gian mạng DPRK đã sử dụng. Các báo cáo này cho phép lực lượng phòng thủ mạng xác định và giảm tiếp xúc với các hoạt động không gian mạng độc hại của DPRK. Trang web CISA có các bản cập nhật mới nhất về các mối đe dọa dai dẳng này: https://www.us-cert.gov/northkorea.

Ngoài ra, CISA cũng cung cấp kiến thức chuyên sâu về an ninh mạng và cơ sở hạ tầng, cùng các cách thực hành cho các bên liên quan, chia sẻ kiến thức đó để tạo điều kiện quản lý rủi ro tốt hơn và áp dụng hành động để bảo vệ các chức năng quan trọng của quốc gia. Dưới đây là các đường liên kết vào các nguồn hỗ trợ của CISA:

- Bảo Vệ Cơ sở Hạ Tầng Quan Trọng: https://www.cisa.gov/protecting-critical-infrastructure
- An Toàn Không Gian Mạng: https://www.cisa.gov/cyber-safety
- Phát Hiện và Phòng Ngừa: https://www.cisa.gov/detection-and-prevention
- Chia sẻ Thông Tin: https://www.cisa.gov/information-sharing-and-awareness
- Nhận Thức CISA: https://www.cisa.gov/insights
- Chống Tội Phạm Mạng: https://www.cisa.gov/combating-cyber-crime
- Các Điều Thiết Yếu về Mạng: https://www.cisa.gov/cyber-essentials
- Mách Bảo: https://www.us-cert.gov/ncas/tips
- Hệ Thống Nhận Thức Mạng Quốc Gia: https://www.us-cert.gov/ncas
- Tư Vấn về Hệ thống Điều khiển Công nghiệp: https://www.us-cert.gov/ics
- Báo cáo Sự cố, Lừa đảo, Phần Mềm Độc hại và Lỗ hổng: https://www.us-cert.gov/report

Báo cáo PIN và FLASH của FBI. Thông báo Công nghiệp Tư nhân (PIN) của FBI cung cấp thông tin cập nhật để nâng cao nhận thức cho lĩnh vực tư nhân về một mối đe dọa mạng đang tiềm ẩn. Các báo cáo Hệ thống Cảnh báo Phối hợp của FBI (FLASH) có thông tin quan trọng do FBI thu thập để một số đối tác cụ thể trong lĩnh vực tư nhân sử dụng. Những thông tin này nhằm cung cấp cho người nhận những thông tin tình báo khả thi để giúp chuyên gia an ninh mạng và quản trị viên mạng chống lại các hành động độc hại dai dẳng của tội phạm mạng. Nếu bạn xác định bất kỳ hoạt động đáng ngờ nào trong doanh nghiệp của bạn hoặc có thông tin liên quan, vui lòng liên hệ với CYWATCH của FBI ngay lập tức. Để có các báo cáo PIN hoặc FLASH liên quan đến mối đe dọa mạng từ DPRK, hãy liên hệ với cywatch@fbi.gov.

- Ban Điều tra Không gian mạng của FBI: https://www.fbi.gov/investigate/cyber
- Chương trình Tùy viên Pháp lý của FBI: Nhiệm vụ cốt lõi của Tùy viên Pháp lý FBI là thiết lập và duy trì liên lạc với lực lượng chấp pháp và an ninh nòng cốt tại một nước ngoài được chỉ định. https://www.fbi.gov/contact-us/legal-attache-offices

Phát hành Thông tin về Phần mềm Độc hại của Lực lượng Không Gian Mạng Hoa Kỳ. Lực lượng không gian mạng của Bộ Quốc Phòng tích cực truy tìm các hoạt động không gian mạng độc hại của DPRK, bao gồm cả phần mềm độc hại của DPRK nhằm khai thác các tổ chức tài chính, tiến hành công tác gián điệp và tạo điều kiện cho các hoạt động mạng độc hại chống lại Hoa Kỳ và các đối tác của Hoa Kỳ. Lực lượng Không Gian Mạng Hoa Kỳ phát hành thông tin định kỳ về phần mềm độc hại, xác định các lỗ hổng cho ngành công nghiệp và chính phủ để bảo vệ cơ sở hạ tầng và mạng trước các hoạt động bất hợp pháp của DPRK. Có thể xem thông tin về phần mềm độc hại, giúp tăng cường an ninh mạng tại các tài khoản Twitter: @US_CYBERCOM và @CNMF_VirusAlert.

Thông tin về Trừng phạt và Tư vấn về Tài chính Bất hợp pháp của Bộ Tài Chính Hoa Kỳ. ***Văn phòng Kiểm soát Tài sản Nước ngoài*** (OFAC) có Trung Tâm Hỗ Trợ cung cấp trực tuyến rất nhiều thông tin liên quan đến các biện pháp trừng phạt DPRK và biện pháp trừng phạt đối với các hoạt động kích hoạt mạng độc hại, bao gồm cả tư vấn trừng phạt, các luật liên quan, Sắc lệnh Hành pháp, quy tắc và quy định liên quan đến các trừng phạt DPRK và trừng phạt có liên quan đến mạng. OFAC cũng đã phát hành một số câu hỏi thường gặp (FAQ) liên quan đến các biện pháp trừng phạt DPRK, các trừng phạt có liên quan đến mạng và tiền kỹ thuật số. Đối với các câu hỏi hoặc thắc mắc liên quan đến các quy định và yêu cầu trừng phạt của OFAC, xin liên hệ Đường Dây Nóng của OFAC, số 1-800-540-6322 hoặc OFAC_Feedback@treasury.gov.

- Trừng Phạt DPRK
  - https://www.treasury.gov/resource-center/sanctions/Programs/pages/nkorea.aspx
  - FAQ - https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_other.aspx#nk
- Trừng Phạt các Hoạt động Mạng Độc hại
  - https://www.treasury.gov/resource-center/sanctions/Programs/pages/cyber.aspx
  - FAQ - https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_other.aspx#cyber
  - FAQ về Tiền Ảo - https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_compliance.aspx#vc_faqs

Mạng lưới Áp dụng Pháp luật với Tội phạm Tài chính (FinCEN) đã phát hành khuyến cáo về vấn đề Triều Tiên sử dụng hệ thống tài chính quốc tế. (https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2017-a008). FinCEN cũng đã phát hành các khuyến cáo cụ thể cho các tổ chức tài chính có nghĩa vụ báo cáo các hoạt động đáng ngờ, cung cấp hướng dẫn về thời điểm và cách thức báo cáo tội phạm mạng và/hoặc hoạt động tội phạm liên quan đến tiền kỹ thuật số:

- Tội phạm Mạng
  - https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2016-a005
- Hoạt động tiền kỹ thuật số bất hợp pháp
  - https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2019-a003
- E-mail của doanh nghiệp bị đột nhập
  - https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2019-a005
  - https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2016-a003

Hội đồng Liên bang Kiểm tra các Tổ chức Tài chính (FFIEC) đã thiết lập Công cụ Đánh giá An Ninh Mạng để giúp các tổ chức tài chính nhận dạng rủi ro và xác định cách đối phó về an ninh mạng. Có thể xem công cụ này tại https://www.ffiec.gov/cyberassessmenttool.htm.

PHỤ LỤC II: Báo cáo của Hội đồng Chuyên gia LHQ về mối Đe dọa Mạng từ DPRK

Báo cáo của Hội đồng Chuyên gia, Ủy Ban Trừng Phạt 1718 của Liên Hợp Quốc đối với DPRK. Ủy ban Trừng phạt 1718 của Hội đồng Bảo An Liên Hiệp Quốc, được sự hỗ trợ của Hội đồng Chuyên gia, đã "thu nhặt, kiểm tra và phân tích thông tin" từ các quốc gia thành viên LHQ, các cơ quan LHQ có liên quan và các bên khác về việc thực hiện các biện pháp được nêu ra trong các Nghị quyết của Hội đồng Bảo An LHQ chống lại Triều Tiên. Hội đồng cũng đưa ra các khuyến nghị về cách tăng cường thực thi các biện pháp trừng phạt, bằng cách cung cấp một Báo cáo Giữa kỳ và một Báo cáo Chung cuộc lên Ủy ban 1718. Những báo cáo này có thể xem tại https://www.un.org/securitycouncil/sanctions/1718/panel_experts/reports.