Khuyến cáo về nhóm gián điệp mạng của Trung Quốc APT40

Kỹ thuật MSS của Trung Quốc đang hoạt động

Australian Government

Australian Signals Directorate

National Cyber
Security Centre
a part of GCHQ

Communications
Security Establishment

**Canadian Centre
for Cyber Security**

Centre de la sécurité
des télécommunications

**Centre canadien
pour la cybersécurité**

Mục lục

Tổng quát

Bối cảnh

Khuyến cáo này, do Trung tâm An ninh Mạng Úc trực thuộc Tổng cục Tín hiệu Úc (ASD's ACSC), Cơ quan An ninh Mạng và Hạ tầng Cơ sở Hoa Kỳ (CISA), Cơ quan An ninh Quốc gia Hoa Kỳ (NSA), Cục Điều tra Liên bang Hoa Kỳ (FBI), Trung tâm An ninh Mạng Quốc gia Vương quốc Anh (NCSC-UK), Trung tâm An ninh Mạng Gia Nã Đại (CCCS), Trung tâm An ninh Mạng Quốc gia Tân Tây Lan (NCSC-NZ), Cơ quan Tình báo Liên bang Đức (BND) và Văn phòng Liên bang Bảo vệ Hiến pháp (BfV), Cơ quan Tình báo Quốc gia Hàn Quốc (NIS) và Trung tâm An ninh mạng Quốc gia trực thuộc NIS, cùng với Trung tâm Sẵn sàng và Chiến lược Đối phó Vấn đề Mạng Quốc gia Nhật Bản (NISC) và Cơ quan Cảnh sát Quốc gia Nhật Bản (NPA) – sau đây được gọi chung là "các cơ quan soạn thảo" – nhằm phác thảo mối đe dọa hiện tại đối với các hệ thống mạng lưới của Úc từ một nhóm tác nhân mạng do nhà nước Cộng hòa Nhân dân Trung Hoa (PRC) bảo trợ. Khuyến cáo này dựa trên sự hiểu biết chung của các cơ quan soạn thảo về mối đe dọa, cũng như các cuộc điều tra đối phó vấn đề do Trung tâm An ninh Mạng Úc trực thuộc Tổng cục Tín hiệu Úc (ASD's ACSC) thực hiện.

Nhóm tác nhân mạng được nhà nước Cộng hòa Nhân dân Trung Hoa (PRC) bảo trợ trước đây đã nhắm vào các tổ chức ở nhiều quốc gia khác nhau, bao gồm cả Úc và Hoa Kỳ, và các kỹ thuật được nêu dưới đây thường xuyên được các tác nhân khác cũng do nhà nước Cộng hòa Nhân dân Trung Hoa bảo trợ sử dụng trên toàn cầu. Do đó, các cơ quan soạn thảo tin rằng nhóm này, cùng với các kỹ thuật tương tự, vẫn là mối đe dọa đối với hệ thống mạng lưới của quốc gia họ.

Các cơ quan soạn thảo đánh giá rằng, nhóm này thực hiện các hoạt động mạng độc hại thay mặt cho Bộ An ninh Quốc gia Trung Quốc (MSS). Các hoạt động và kỹ thuật của nhóm này trùng lặp với những nhóm đang được theo dõi mang tên 'Mối Đe dọa Liên tục Nâng cao 40' (Advanced Persistent Threat - APT 40) (còn được biết đến với các tên gọi khác như Kryptonite Panda, GINGHAM TYPHOON, Leviathan và Bronze Mohawk trong các phúc trình của ngành). Nhóm này trước đây đã được trình báo có trụ sở tại Hải Khẩu, tỉnh Hải Nam, Cộng hòa Nhân dân Trung Hoa (PRC) và nhận nhiệm vụ từ Bộ An ninh Quốc gia Trung Quốc (MSS), cụ thể là Bộ An ninh Quốc gia tỉnh Hải Nam.[2] Khuyến cáo sau đây đưa ra một số ví dụ điển hình về các kỹ thuật mà đối tượng này đã sử dụng trong thực tế đối với hai hệ thống mạng lưới của nạn nhân. Các trường hợp nghiên cứu điển hình này có ý nghĩa quan trọng đối với các chuyên gia an ninh mạng trong việc nhận ra, ngăn chặn và khắc phục các cuộc xâm nhập do nhóm APT40 thực hiện nhắm vào hệ thống mạng lưới của chính họ. Các trường hợp nghiên cứu điển hình được chọn, là những nghiên cứu đã thực hiện biện pháp khắc phục phù hợp, giúp giảm nguy cơ bị tác nhân này, hoặc những tác nhân khác tái khai thác. Do đó, các trường hợp nghiên cứu điển hình thường là cũ hơn để bảo đảm các tổ chức có đủ thời gian cần thiết để khắc phục.

Tóm tắt hoạt động

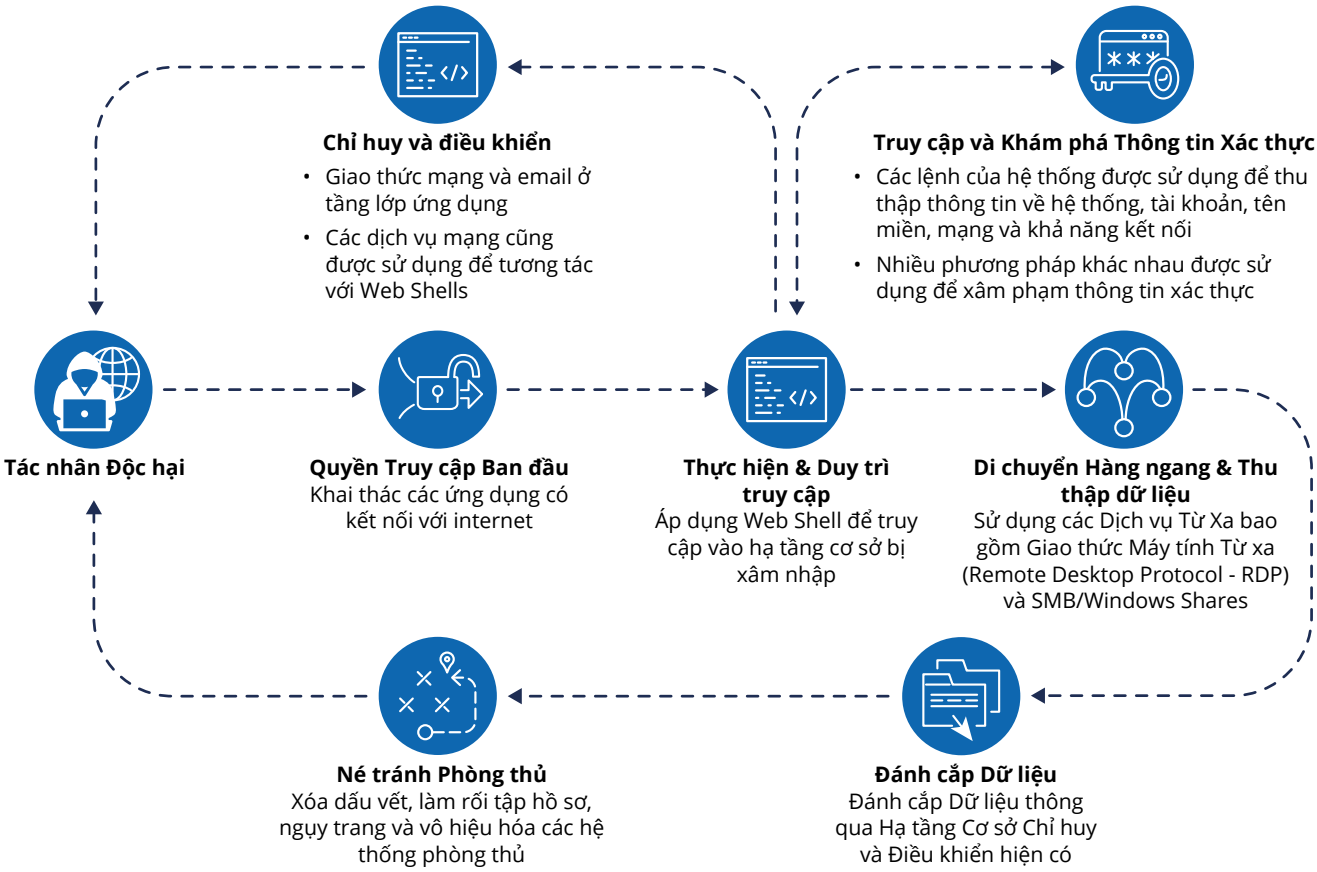
Nhóm APT40 đã nhiều lần nhắm vào các hệ thống mạng lưới của Úc cũng như các hệ thống mạng lưới của chính phủ và lãnh vực tư nhân trong khu vực, và mối đe dọa mà chúng gây ra cho các hệ thống mạng lưới của chúng ta vẫn đang tiếp diễn. Các kỹ thuật được mô tả trong bản khuyến cáo này vẫn được sử dụng thường xuyên đối với các hệ thống mạng lưới của Úc.

Đáng chú ý, APT40 có khả năng nhanh chóng chuyển đổi và thích ứng để khai thác Chứng-minh Khái-niệm (là một sự chứng minh cho thấy một lỗ hổng hoặc điểm yếu bảo mật có thể bị khai thác - Proof-of-concept - POC) về các lỗ hổng mới, và ngay lập tức sử dụng chúng để tấn công các hệ thống mạng lưới mục tiêu sở hữu hạ tầng cơ sở của lỗ hổng đó. APT40 thường xuyên tiến hành dò thám các hệ thống mạng lưới họ để ý tới, bao gồm cả các hệ thống mạng lưới tại quốc gia của các cơ quan soạn thảo, nhằm tìm kiếm cơ hội xâm nhập mục tiêu. Việc dò thám thường xuyên giúp nhóm này xác định các thiết bị nào dễ bị tấn công, đã hết hạn sử dụng, hoặc không còn được bảo trì trên các hệ thống mạng lưới đáng quan tâm và nhanh chóng khai thác các lỗ hổng đó. APT40 liên tục thành công trong việc khai thác các lỗ hổng kể từ đầu năm 2017.

APT40 nhanh chóng khai thác các lỗ hổng vừa được công bố trong những phần mềm phổ biến như Log4J (CVE-2021-44228), Atlassian Confluence (CVE-2021-31207, CVE-2021-26084) và Microsoft Exchange (CVE-2021-31207; CVE-2021-34523; CVE-2021-34473). Trung tâm An ninh Mạng Úc trực thuộc Tổng cục Tín hiệu Úc (ASD's ACSC) và các cơ quan soạn thảo dự đoán rằng nhóm này sẽ tiếp tục sử dụng POC cho những lỗ hổng nghiêm trọng mới trong vòng vài giờ, hoặc vài ngày sau khi lỗ hổng được công bố rộng rãi.

2 Bộ Tư pháp Hoa Kỳ. Năm 2021. Bốn Công dân Trung Quốc Làm việc với Bộ An ninh Quốc gia bị Buộc tội trong Chiến dịch Xâm nhập Máy Vi tính Toàn cầu Nhắm vào Sở hữu Trí tuệ và Thông tin Kinh doanh Bí mật, Bao gồm các Nghiên cứu về Bệnh Truyền nhiễm.

Hình 1. Sơ đồ luồng TTP (Chiến thuật, Kỹ thuật và Phương sách) cho hoạt động của nhóm APT40



Nhóm này có vẻ ưa thích việc khai thác các hạ tầng cơ sở công khai có lỗ hổng, hơn là sử dụng các kỹ thuật đòi hỏi sự tương tác của người sử dụng, chẳng hạn như các chiến dịch lừa đảo qua email (phishing). Họ cũng đặt ưu tiên cao cho việc thu thập thông tin xác thực hợp lệ để giúp cho nhiều hoạt động tiếp theo. APT40 thường xuyên sử dụng web shells (là một tập lệnh độc hại được tải lên máy chủ mạng, cấp cho kẻ tấn công quyền điều khiển từ xa) (T1505.003) để duy trì quyền truy cập lâu dài, đặc biệt là vào giai đoạn đầu của vòng đời xâm nhập. Thông thường, sau khi truy cập ban đầu thành công, APT40 tập trung vào việc đặt nền móng để duy trì quyền truy cập vào môi trường của nạn nhân. Tuy nhiên, vì quá trình duy trì quyền truy cập lâu dài diễn ra ở giai đoạn đầu của một cuộc xâm nhập, do đó nó có thể bị phát hiện trong hầu hết các vụ tấn công – bất kể mức độ bị xâm phạm, hay các thực hành tiếp theo có được thực hiện hay không.

Kỹ thuật tấn công đáng chú ý

Mặc dù trước đây APT40 đã sử dụng các trang mạng của Úc đã bị xâm nhập làm máy chủ chỉ huy và điều khiển (C2) cho các hoạt động của mình, nhóm này giờ đây đã thích nghi và biến đổi kỹ thuật này (T1594).

APT40 đã nắm bắt xu hướng toàn cầu trong việc sử dụng các thiết bị bị xâm nhập, bao gồm cả các thiết bị cho văn-phòng-nhỏ, hoặc văn-phòng-tại-nhà (small-office/home-office - SOHO), làm hạ tầng cơ sở hoạt động và các bộ chuyển-hướng cuối-cùng (last-hop redirectors) (T1584.008) cho các hoạt động tại Úc. Xu hướng này đã giúp các cơ quan soạn thảo xác định rõ hơn và theo dõi các hoạt động của nhóm này.

Nhiều thiết bị SOHO này đã hết vòng đời sử dụng, hoặc chưa được cập nhật bản vá, trở thành mục tiêu dễ bị khai thác bằng kỹ thuật N-day. Một khi bị xâm nhập, các thiết bị SOHO trở thành điểm khởi đầu cho các cuộc tấn công được thiết kế để hòa nhập với lưu lượng hợp pháp, gây khó khăn cho các chuyên gia bảo vệ có nhiệm vụ bảo vệ hệ thống mạng lưới (T1001.003).

Kỹ thuật này cũng thường xuyên được các nhóm tác nhân khác cũng do nhà nước Trung Quốc tài trợ trên toàn cầu sử dụng, và các cơ quan tác giả xem đây là một mối đe dọa chung. Để biết thêm thông tin, xin hãy tham khảo các khuyến cáo chung Các Tác nhân Mạng do Nhà nước Cộng hòa Nhân dân Trung Hoa Tài trợ Khai thác Nhà Cung cấp Hệ thống mạng lưới và Thiết bị và Các Tác nhân do Nhà nước Cộng hòa Nhân dân Trung Hoa Bảo trợ Xâm nhập và Duy trì Quyền Truy cập vào Hạ tầng Cơ sở Thiết yếu của Hoa Kỳ.

APT40 cũng thỉnh thoảng sử dụng hạ tầng cơ sở thuê, hoặc mua làm hạ tầng cơ sở chỉ huy và điều khiển C2 nhắm vào nạn nhân trong các hoạt động của họ; tuy nhiên, kỹ thuật này dường như đang có xu hướng giảm đi.

Công cụ

Trung tâm An ninh Mạng Úc trực thuộc Tổng cục Tín hiệu Úc (ASD's ACSC) đang chia sẻ một số hồ sơ độc hại được xác định trong các cuộc điều tra được nêu dưới đây. Các tập hồ sơ này đã được tải lên VirusTotal (VirusTotal - là dịch vụ trực tuyến miễn phí phân tích các tập hồ sơ và URL đáng nghi ngờ để phát hiện phần mềm độc hại và nội dung độc hại khác) nhằm giúp cộng đồng phòng thủ hệ thống mạng lưới, và an ninh hệ thống mạng lưới rộng lớn hơn hiểu rõ hơn về các mối đe dọa mà họ cần phòng chống.

Nghiên cứu trường hợp điển hình

Trung tâm An ninh Mạng Úc trực thuộc Tổng cục Tín hiệu Úc (ASD's ACSC) đang chia sẻ hai phúc trình điều tra đã được ẩn danh nhằm nâng cao nhận thức về phương thức các tác nhân sử dụng công cụ, và kỹ thuật tấn công của chúng.

MD5	Tên của tập hồ sơ	Thông tin bổ sung
26a5a7e71a601be991073c78d513dee3	horizon.jsp	1 kB | Mã nguồn Java
87c88f06a7464db2534bc78ec2b915de	Index_jsp$ProxyEndpoint$Attach.class	597 B | Java Bytecode (là một ngôn ngữ trung gian được tạo ra từ mã nguồn Java)
6a9bc68c9bc5cefaf1880ae6ffb1d0ca	Index_jsp.class	5 kB | Java Bytecode
64454645a9a21510226ab29e01e76d39	Index_jsp.java	5 kB | Mã nguồn Java
e2175f91ce3da2e8d46b0639e941e13f	Index_jsp$ProxyEndpoint.class	4 kB | Java Bytecode
9f89f069466b8b5c9bf25c9374a4daf8	Index_jsp$ProxyEndpoint$1.class	3 kB | Java Bytecode
187d6f2ed2c80f805461d9119a5878ac	Index_jsp$ProxyEndpoint$2.class	1 kB | Java Bytecode
ed7178cec90ed21644e669378b3a97ec	Nova_jsp.class	7 kB | Java Bytecode
5bf7560d0a638e34035f85cd3788e258	Nova_jsp$TomcatListenerMemShellFromThread.class	8 kB | Java Bytecode
e02be0dc614523ddd7a28c9e9d500cff	Nova_jsp.java	15 kB | Mã nguồn Java

Nghiên cứu trường hợp điển hình 1

Phúc trình này đã được ẩn danh nhằm cho phép phổ biến rộng rãi hơn. Tổ chức bị ảnh hưởng kể từ đây được gọi là 'tổ chức'. Một số chi tiết cụ thể đã được lược bỏ để bảo vệ danh tính của nạn nhân và các phương pháp đối phó vấn đề của Trung tâm An ninh Mạng Úc trực thuộc Tổng cục Tín hiệu Úc (ASD's ACSC).

Bản tóm tắt chính

Phúc trình này trình bày các phát hiện từ cuộc điều tra của Trung tâm An ninh Mạng Úc trực thuộc Tổng cục Tín hiệu Úc (ASD's ACSC) về việc hệ thống mạng lưới của tổ chức đã bị xâm nhập trong khoảng thời gian từ tháng 7 đến tháng 9 năm 2022. Phúc trình điều tra này đã được cung cấp cho tổ chức nhằm tóm tắt các hoạt động độc hại được quan sát thấy và đưa ra các khuyến cáo để khắc phục. Các phát hiện cho thấy vụ xâm nhập là do nhóm APT40.

Vào giữa tháng 8, Trung tâm An ninh Mạng Úc trực thuộc Tổng cục Tín hiệu Úc (ASD's ACSC) đã thông báo cho tổ chức về các tương tác độc hại với hệ thống mạng lưới của họ, các tương tác này có thể xuất phát từ một thiết bị bị xâm nhập mà nhóm này sử dụng vào cuối tháng 8. Với sự đồng ý của tổ chức, Trung tâm An ninh Mạng Úc trực thuộc Tổng cục Tín hiệu Úc (ASD's ACSC) đã triển khai các thiết bị cảm biến dựa trên máy chủ (host-based sensors) cho các máy chủ có thể đã bị ảnh hưởng trong hệ thống mạng lưới của tổ chức. Các thiết bị cảm biến này giúp các nhà phân tích để đối phó với vấn đề của Trung tâm An ninh Mạng Úc trực thuộc Tổng cục Tín hiệu Úc (ASD's ACSC) thực hiện một cuộc điều tra 'pháp y kỹ thuật số' toàn diện. Sử dụng dữ liệu cảm biến có sẵn, các nhà phân tích của Trung tâm An ninh Mạng Úc trực thuộc Tổng cục Tín hiệu Úc (ASD's ACSC) đã thiết kế ra bản đồ hoạt động của nhóm này, và tạo ra một dòng thời gian chi tiết về các sự kiện được quan sát thấy.

Từ tháng 7 đến tháng 8, hoạt động của các tác nhân chính được Trung tâm An ninh Mạng Úc trực thuộc Tổng cục Tín hiệu Úc (ASD's ACSC) quan sát thấy bao gồm:

- xác định máy chủ (host enumeration), cho phép tác nhân tự thiết kế bản đồ mạng của riêng mình;
- sử dụng web shell, tác nhân đã lấy được điểm truy cập ban đầu vào hệ thống mạng lưới và khả năng thực hiện lệnh; và
- triển khai các công cụ khác cho các mục đích độc hại.

Cuộc điều tra đã phát hiện bằng chứng cho thấy một lượng lớn dữ liệu nhạy cảm đã bị truy cập, cùng với bằng chứng cho thấy các tác nhân đã di chuyển hàng ngang trong hệ thống mạng lưới (T1021.002). Phần lớn cuộc xâm nhập được thực hiện dễ dàng vì nhóm này áp dụng nhiều phương pháp (vector) truy cập vào hệ thống mạng lưới, do cấu trúc mạng bằng phẳng, và việc sử dụng phần mềm phát triển nội bộ không an toàn có thể được sử dụng để tải lên các tập hồ sơ tùy ý. Dữ liệu bị lấy đi bao gồm thông tin xác thực đặc quyền cho phép nhóm đăng nhập, cũng như thông tin hệ thống mạng lưới cho phép các tác nhân lấy lại quyền truy cập trái phép nếu phương thức truy cập ban đầu bị ngăn chặn. Ngoài những công cụ đã có trên máy bị khai thác ban đầu, không phát hiện thêm công cụ độc hại nào khác; tuy nhiên, việc nhóm này có quyền truy cập vào các thông tin xác thực hợp lệ và có đặc quyền, cho thấy họ không cần đến công cụ hỗ trợ nào khác. Kết luận từ cuộc điều tra cho thấy tổ chức này rất có thể đã bị APT40 cố tình nhắm vào, thay vì trở thành nạn nhân một cách tình cờ do một lỗ hổng đã được công bố rộng rãi.

Kết quả điều tra

Vào giữa tháng 8 năm 2022, Trung tâm An ninh Mạng Úc trực thuộc Tổng cục Tín hiệu Úc (ASD's ACSC) đã thông báo cho tổ chức là một địa chỉ IP độc hại được xác nhận có thể có liên quan đến một nhóm tấn công mạng do nhà nước bảo trợ, địa chỉ IP độc hại đã tương tác với hệ thống mạng lưới máy vi tính của tổ chức trong khoảng thời gian ít nhất từ tháng 7 đến tháng 8. Thiết bị bị xâm nhập có thể thuộc về một doanh nghiệp nhỏ hoặc người sử dụng tại nhà.

Vào cuối tháng 8, Trung tâm An ninh Mạng Úc trực thuộc Tổng cục Tín hiệu Úc (ASD's ACSC) đã triển khai một phần mềm chuyên dụng dựa trên máy chủ đến các máy chủ trên hệ thống mạng lưới của tổ chức, và đưa ra bằng chứng về việc bị ảnh hưởng bởi sự xâm phạm.

Một số dữ liệu (artefacts) có thể hữu ích cho quá trình điều tra đã không có sẵn do cấu hình nhật ký ghi chép (là quá trình ghi chép lại các sự kiện xảy ra trong hệ thống máy tính hoặc mạng – logging) hoặc do thiết kế hệ thống mạng lưới của tổ chức. Mặc dù vậy, do sự sẵn sàng của tổ chức trong việc cung cấp tất cả dữ liệu hiện có, đã giúp các chuyên gia đối phó vấn đề của Trung tâm An ninh Mạng Úc trực thuộc Tổng cục Tín hiệu Úc (ASD's ACSC) thực hiện phân tích toàn diện, và đưa ra nhận xét về các hoạt động có thể là do APT40 thực hiện trên hệ thống mạng lưới của tổ chức.

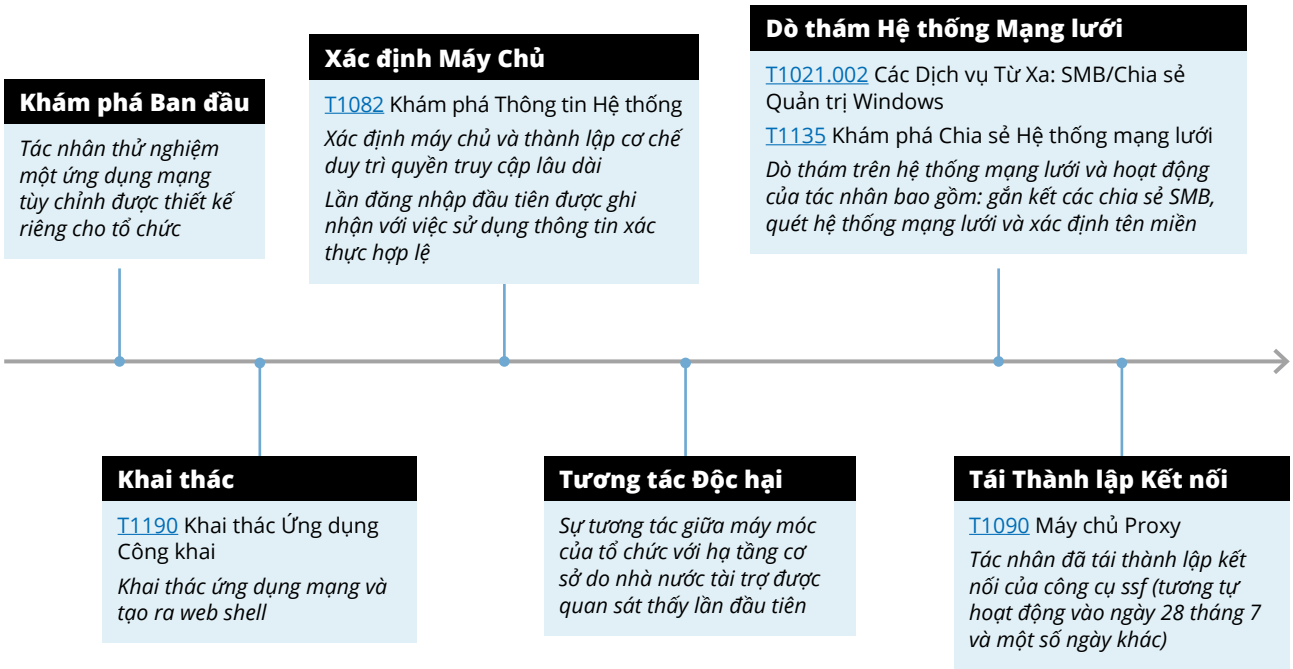
Vào tháng 9, sau khi được Trung tâm An ninh Mạng Úc trực thuộc Tổng cục Tín hiệu Úc (ASD's ACSC) cố vấn, tổ chức đã quyết định đưa địa chỉ IP được xác định trong thông báo ban đầu vào danh sách ngăn chặn (denylist). Đến tháng 10, tổ chức bắt đầu đưa ra các biện pháp khắc phục.

Chi tiết

Bắt đầu từ tháng 7, tác nhân đã có thể thử nghiệm và khai thác một ứng dụng mạng tùy chỉnh (T1190) chạy trên `<webapp>2-ext`, cho phép nhóm này thành lập một vị trí trong khu vực 'phi quân sự mạng' (demilitarized zone - DMZ). Vị trí này được tận dụng để xác định cả hệ thống mạng lưới cũng như tất cả các miền có thể nhìn thấy. Thông tin xác thực bị xâm phạm (T1078.002) đã được sử dụng để truy vấn Active Directory (Thư mục Hoạt động) (T1018) và đánh cắp dữ liệu bằng cách gắn kết các chia sẻ hồ sơ (file shares) (T1039) từ nhiều máy trong vùng DMZ. Tác nhân đã thực hiện một cuộc tấn công Kerberoasting (Kerberoasting là một kỹ thuật tấn công sau khi khai thác) nhằm lấy được thông tin xác thực hợp lệ trong hệ thống mạng lưới từ một máy chủ (T1558.003). Không thấy nhóm tác nhân này thành lập thêm bất kỳ điểm hiện diện nào khác trong cả vùng DMZ lẫn hệ thống mạng lưới nội bộ.

Minh hoạ dòng thời gian

Dòng thời gian dưới đây cho thấy tổng quát về các giai đoạn chính trong hoạt động của tác nhân được ghi nhận trên hệ thống mạng lưới của tổ chức.



Chi tiết của dòng thời gian

Tháng 7: Tác nhân đã thành lập kết nối ban đầu tới trang chính của một ứng dụng mạng tùy chỉnh (T1190) được thiết kế riêng cho tổ chức (kể từ đây sẽ được gọi là "ứng dụng mạng" hoặc '*webapp*') thông qua một kết nối bảo mật tầng lớp truyền tải (TLS) (T1102). Không có hoạt động đáng chú ý nào khác được ghi nhận thêm.

Tháng 7: Tác nhân bắt đầu xác định các điểm cuối (endpoints) của trang mạng ứng dụng để tiến hành điều tra thêm[2].

Tháng 7: Tác nhân tập trung vào việc cố gắng khai thác một điểm cuối cụ thể.

Tháng 7: Tác nhân đã gởi yêu cầu thành công `POST (Kiểm tra tự động khi bật nguồn)` tới máy chủ mạng, có thể là thông qua một web shell được đặt trên một trang khác. Một địa chỉ IP thứ hai, có thể cũng do cùng nhóm tác nhân sử dụng, bắt đầu gửi yêu cầu đến cùng một URL. Tác nhân đã tạo ra và thử nghiệm một số được cho là web shell.

Phương thức khai thác chính xác hiện chưa được xác định, nhưng rõ ràng rằng điểm cuối cụ thể đã bị nhắm tới để tạo ra các tập hồ sơ trên `<webapp>2-ext`.

Trung tâm An ninh Mạng Úc trực thuộc Tổng cục Tín hiệu Úc (ASD's ACSC) cho rằng kết nối từ 2 địa chỉ IP này là một phần của cùng một vụ xâm nhập, do chúng có chung lợi ích và các kết nối ban đầu xảy ra chỉ cách nhau vài phút.

Tháng 7: Nhóm này tiếp tục thực hiện dò quét xác định máy chủ, tìm kiếm cơ hội để chiếm đặc quyền nâng cao trong hệ thống và triển khai một web shell khác. Các tác nhân đăng nhập vào ứng dụng mạng bằng thông tin xác thực đã bị đánh cắp cho `<firstname.surname>@<organisation domain>`.

Hoạt động của các tác nhân dường như đã thất bại trong việc dành chiếm đặc quyền nâng cao trong hệ thống trên `<webapp>2-ext`. Thay vào đó, tác nhân đã chuyển sang các hoạt động dựa trên hệ thống mạng lưới.

Tháng 7: Tác nhân thử nghiệm thông tin xác thực đã bị đánh cắp của một tài khoản dịch vụ [3] mà tác nhân này có thể tìm thấy đã được mã hóa cứng (đề cập đến việc cấy các giá trị hoặc dữ liệu cụ thể trực tiếp vào mã nguồn của chương trình – hardcoded) trong các tập hồ sơ nhị phân có thể truy cập nội bộ.

Tháng 7: Tác nhân triển khai công cụ mã nguồn mở Ổ cắm Chuyển tiếp An toàn (là một công cụ mạng cho phép chuyển tiếp dữ liệu một cách an toàn từ nhiều ổ cắm - Secure Socket Funnelling), được sử dụng để kết nối ra với hạ tầng cơ sở độc hại. Kết nối này được dùng để chuyển tiếp lưu lượng từ các máy tấn công của tác nhân vào hệ thống mạng lưới nội bộ của tổ chức, nơi tên của các máy bị lộ ra trong nhật ký ghi chép sự kiện khi họ cố gắng sử dụng thông tin xác thực của tài khoản dịch vụ.

Tháng 8: Tác nhân được quan sát thấy thực hiện một số hoạt động thưa thớt, bao gồm việc thành lập các kết nối liên quan đến tài khoản dịch vụ, nhưng đã bị thất bại.

Tháng 8: Tác nhân thực hiện việc rà quét và xác định thông tin hệ thống mạng lưới cũng như Thư mục Hoạt động một cách đáng kể. Một tài khoản bị đánh cắp khác sau đó được sử dụng để gắn các ổ chia sẻ trên các máy của Windows trong vùng DMZ nhằm giúp cho việc đánh cắp dữ liệu được thành công.

Đây có vẻ là hành vi khai thác cơ hội khi sử dụng thông tin xác thực bị đánh cắp trên các máy có thể gắn kết trong DMZ. Tường lửa đã ngăn chặn tác nhân không để cho họ thực hiện hoạt động tương tự trong hệ thống mạng lưới nội bộ.

Tháng 8 – Tháng 9: Công cụ SSF đã tái thành lập kết nối đến một địa chỉ IP độc hại. Nhóm này không thực hiện bất kỳ hoạt động bổ sung nào cho đến khi quyền truy cập của họ bị ngăn chặn.

Tháng 9: Tổ chức đã ngăn chặn địa chỉ IP độc hại bằng cách đưa vào danh sách ngăn chặn trên tường lửa của họ.

2 Trong ngữ cảnh này, một điểm cuối (endpoint) là một chức năng của ứng dụng mạng.

3 Tài khoản dịch vụ không gắn liền với cá nhân người sử dụng, nhưng được liên kết với các dịch vụ. Trong một miền doanh nghiệp của Microsoft, có nhiều loại tài khoản khác nhau.

4 Việc gắn kết các ổ chia sẻ là quá trình cho phép người sử dụng, hoặc nhóm người sử dụng truy cập các tập hồ sơ trong cấu trúc hệ thống hồ sơ.

Chiến thuật và kỹ thuật của tác nhân

Khung làm việc MITRE ATT&CK là một bộ sưu tập tài liệu về các chiến thuật và kỹ thuật được tác nhân sử dụng trong không gian mạng. Khung làm việc này là do tổ chức phi lợi nhuận của Mỹ – MITRE Corporation tạo ra, và hoạt động như một ngôn ngữ chung toàn cầu về hành vi của tác nhân.

Trung tâm An ninh Mạng Úc trực thuộc Tổng cục Tín hiệu Úc (ASD's ACSC) đánh giá các kỹ thuật và chiến thuật sau đây có liên quan đến hoạt động độc hại của tác nhân:

Dò thám

T1594 – Tìm kiếm các Trang Mạng thuộc Sở hữu của Nạn nhân

Tác nhân đã thực hiện việc xác định trang mạng của ứng dụng mạng tùy chỉnh để tìm các cơ hội truy cập vào hệ thống mạng lưới.

Quyền Truy cập Ban đầu

T1190 – Khai thác Ứng dụng Công khai (liên quan đến việc khai thác ứng dụng mạng tùy chỉnh)

T1078.002 – Tài khoản Hợp lệ: Tài khoản Miền (liên quan đến việc đăng nhập bằng thông tin xác thực bị đánh cắp)

Việc khai thác các ứng dụng mạng tùy chỉnh có kết nối với internet, đã cung cấp điểm truy cập ban đầu cho tác nhân. Sau đó, tác nhân có thể sử dụng thông tin đăng nhập mà chúng đã đánh cắp để tiếp tục truy cập vào hệ thống mạng lưới.

Thực hiện

T1059 – Trình Thông dịch Lệnh và Tập lệnh (liên quan đến việc thực hiện mệnh lệnh thông qua web shell)

T1072 – Công cụ Triển khai Phần mềm (liên quan đến việc tác nhân sử dụng công cụ mã nguồn mở Ổ cắm Chuyển tiếp An toàn (Secure Socket Funnelling -SSF) để kết nối với một IP)

Duy trì truy cập

T1505.003 – Thành phần Phần mềm Máy chủ: Web Shell (liên quan đến việc sử dụng web shell và SSF để thành lập quyền truy cập)

Quyền Truy cập Thông tin Xác thực

T1552.001 – Thông tin Xác thực từ Kho Lưu trữ Mật mã (liên quan đến các tập hồ sơ mật mã liên quan đến hệ thống quản lý tòa nhà (BMS))

T1558.003 – Ăn cắp hoặc Làm Giả Vé Kerberos: Kerberoasting (liên quan đến cuộc tấn công nhằm lấy thông tin xác thực hệ thống mạng lưới)

Di chuyển hàng ngang trong hệ thống

T1021.002 – Dịch vụ Từ Xa: Chia sẻ SMB (liên quan đến việc tác nhân gắn kết các chia sẻ SMB từ nhiều thiết bị)

Thu thập dữ liệu

T1213 – Dữ liệu từ Kho Thông tin (liên quan đến các hướng dẫn/tài liệu tìm thấy trên máy chủ BMS)

Đánh cắp dữ liệu

T1041 – Đánh cắp dữ liệu thông qua kênh Chỉ huy và Điều khiển C2 (liên quan đến việc tác nhân đánh cắp dữ liệu từ Active Directory và các ổ chia sẻ được gắn kết)

Nghiên cứu điển hình 2

Phúc trình này đã được ẩn danh nhằm cho phép phổ biến rộng rãi hơn. Tổ chức bị ảnh hưởng kể từ đây được gọi là 'tổ chức'. Một số chi tiết cụ thể đã được lược bỏ để bảo vệ danh tính của nạn nhân và các phương pháp đối phó vấn đề của Trung tâm An ninh Mạng Úc trực thuộc Tổng cục Tín hiệu Úc (ASD's ACSC).

Bản tóm tắt chính

Phúc trình này trình bày các kết quả điều tra của Trung tâm An ninh Mạng Úc trực thuộc Tổng cục Tín hiệu Úc (ASD's ACSC) về việc mạng của tổ chức đã bị xâm nhập vào tháng 4 năm 2022. Tổ chức đã được cung cấp phúc trình điều tra này với mục đích tóm tắt các hoạt động độc hại đã được quan sát thấy và đưa ra các khuyến cáo để khắc phục. Cuộc điều tra cho thấy vụ xâm nhập là do nhóm APT40 thực hiện.

Vào tháng 5 năm 2022, Trung tâm An ninh Mạng Úc trực thuộc Tổng cục Tín hiệu Úc (ASD's ACSC) đã thông báo cho một tổ chức về hoạt động độc hại nghi ngờ đã ảnh hưởng đến hệ thống mạng lưới của tổ chức kể từ tháng 4 năm 2022. Sau đó, tổ chức này đã thông báo cho Trung tâm An ninh Mạng Úc trực thuộc Tổng cục Tín hiệu Úc (ASD's ACSC) là họ đã phát hiện phần mềm độc hại trên một máy chủ có kết nối với internet. Máy chủ này cung cấp cổng đăng nhập cho việc tìm giải pháp truy cập từ xa vào hệ thống doanh nghiệp của tổ chức. Máy chủ này sử dụng một sản phẩm quản lý danh tính và đăng nhập truy cập từ xa và sẽ được đề cập đến trong phúc trình này là "thiết bị bị xâm nhập". Phúc trình này trình bày chi tiết các phát hiện từ cuộc điều tra, và các khuyến cáo khắc phục được thiết kế riêng cho tổ chức dựa trên cuộc điều tra do Trung tâm An ninh Mạng Úc trực thuộc Tổng cục Tín hiệu Úc (ASD's ACSC).

Bằng chứng cho thấy một phần hệ thống mạng lưới của tổ chức đã bị xâm nhập bởi tác nhân mạng thông qua cổng đăng nhập truy cập từ xa của tổ chức, ít nhất là từ tháng 4 năm 2022. Máy chủ này có thể đã bị nhiều tác nhân khác nhau xâm nhập, và rất có thể đã bị ảnh hưởng bởi một lỗ hổng cho việc thực hiện mã từ xa (RCE) đã được công bố rộng rãi vào thời điểm xảy ra sự xâm phạm.

Các hoạt động chính của tác nhân mà Trung tâm An ninh Mạng Úc trực thuộc Tổng cục Tín hiệu Úc (ASD's ACSC) nhận thấy được, bao gồm:

- xác định máy chủ, cho phép tác nhân thiết kế bản đồ riêng về hệ thống mạng lưới;
- khai thác các ứng dụng có kết nối với internet và sử dụng web shell, việc này giúp tác nhân tạo ra chỗ đứng ban đầu trong hệ thống mạng lưới và có khả năng thực hiện lệnh;
- khai thác lỗ hổng phần mềm để đạt được đặc quyền nâng cao; và
- thu thập thông tin đăng nhập giúp cho việc di chuyển hàng ngang

Trung tâm An ninh Mạng Úc trực thuộc Tổng cục Tín hiệu Úc (ASD's ACSC) phát hiện ra một tác nhân độc hại đã đánh cắp hàng trăm cặp tên người sử dụng và mật mã trên thiết bị bị xâm nhập vào tháng 4 năm 2022, cùng với một số mã xác thực đa yếu tố (multi-factor authentication codes) và các dữ liệu kỹ thuật (technical artefacts) liên quan đến các phiên truy cập từ xa. Sau cuộc kiểm tra nội bộ, tổ chức đã xác định mật mã là hợp lệ. Trung tâm An ninh Mạng Úc trực thuộc Tổng cục Tín hiệu Úc (ASD's ACSC) nhận xét rằng tác nhân có thể đã thu thập các dữ liệu kỹ thuật này để chiếm đoạt hoặc tạo ra phiên đăng nhập từ xa với tư cách là người sử dụng hợp pháp, và truy cập vào hệ thống mạng lưới nội bộ của tổ chức bằng tài khoản người sử dụng hợp pháp.

Kết quả điều tra

Tóm tắt điều tra

Trung tâm An ninh Mạng Úc trực thuộc Tổng cục Tín hiệu Úc (ASD's ACSC) xác định là tác nhân đã xâm nhập vào thiết bị được sử dụng để cung cấp phiên đăng nhập từ xa cho nhân viên của tổ chức và lợi dụng việc xâm nhập này để tiến hành thêm các hoạt động khác. Các thiết bị này bao gồm ba máy chủ có trách nhiệm cân bằng các yêu cầu thông tin (load-balanced hosts), là nơi phát hiện ra bằng chứng xâm phạm sớm nhất. Tổ chức đã tắt hai trong ba máy chủ này ngay sau khi phát hiện ra vụ xâm nhập ban đầu. Kết quả là, tất cả các hoạt động tiếp theo đều diễn ra trên một máy chủ duy nhất. Các máy chủ khác có liên quan đến thiết bị bị xâm nhập, các yêu cầu thông tin cũng được cân bằng theo cách tương tự. Để dễ hiểu, toàn bộ các thiết bị bị xâm nhập sẽ được gọi chung là "một thiết bị" trong phần lớn nội dung của phúc trình này.

Tác nhân bị tình nghi là đã lợi dụng các lỗ hổng bảo mật được công khai để triển khai web shell vào thiết bị bị xâm nhập từ tháng 4 năm 2022 trở đi. Tác nhân thuộc nhóm này được cho rằng đã đạt được đặc quyền truy cập nâng cao trên thiết bị. Trung tâm An ninh Mạng Úc trực thuộc Tổng cục Tín hiệu Úc (ASD's ACSC) không thể xác định đầy đủ mức độ hoạt động do không có đầy đủ các dữ liệu của nhật ký ghi chép. Tuy nhiên, bằng chứng trên thiết bị cho thấy tác nhân đã thực hiện được những điều sau đây:

- Thu thập hàng trăm cặp tên người sử dụng và mật mã hợp lệ; và
- Các dữ liệu kỹ thuật thu thập được có thể cho phép tác nhân truy cập vào hạ tầng cơ sở ảo của máy vi tính để bàn (VDI) dưới danh nghĩa một người sử dụng hợp pháp.

Trung tâm An ninh Mạng Úc trực thuộc Tổng cục Tín hiệu Úc (ASD's ACSC) đánh giá rằng tác nhân có thể đã tìm cách mở rộng mức độ xâm nhập vào hệ thống mạng lưới của tổ chức. Các dữ liệu kỹ thuật bị tác nhân đánh cắp, có thể đã cho phép họ chiếm quyền hoặc tạo ra các phiên làm việc trên máy vi tính ảo để bàn dưới danh nghĩa người sử dụng hợp pháp, có thể là người sử dụng mà họ chọn lựa, bao gồm cả quản trị viên. Tác nhân có thể đã sử dụng phương thức truy cập này để tiếp tục xâm nhập các dịch vụ của tổ chức nhằm đạt được quyền truy cập lâu dài và các mục tiêu khác.

Các thiết bị khác của tổ chức do nhà cung cấp dịch vụ lưu trữ quản lý không có dấu hiệu bị xâm nhập.

Quyền truy cập

Máy chủ chứa thiết bị bị xâm nhập cung cấp chức năng xác thực thông qua thư mục hoạt động (Active Directory) và máy chủ mạng (webserver), dành cho người sử dụng kết nối tới các phiên làm việc trên máy tính ảo để bàn (T1021.001).

Vị trí	Tên máy chủ thiết bị bị xâm nhập (để cân bằng các yêu cầu thông tin)
Trung tâm Dữ liệu 1	HOST1, HOST2, HOST3

Hạ tầng cơ sở thiết bị cũng bao gồm các cổng truy cập của máy chủ (access gateway) cung cấp đường hầm tới VDI cho người sử dụng, một khi họ có mã xác thực (authentication token) được tạo ra và tải xuống từ thiết bị.

Không có bằng chứng nào cho thấy các máy chủ này bị xâm nhập. Tuy nhiên, nhật ký ghi chép các cổng truy cập của máy chủ, lại cho thấy có sự tương tác đáng kể với các địa chỉ IP độc hại đã được biết đến. Rất có thể điều này phản ánh hoạt động đã diễn ra trên máy chủ này, hoặc các kết nối hệ thống mạng lưới với hạ tầng cơ sở của tác nhân đã tiếp cận máy chủ này. Mục đích của hoạt động này không thể được xác định rõ ràng dựa trên bằng chứng hiện có, nhưng cho thấy nhóm này đã cố gắng di chuyển hàng ngang trong hệ thống mạng lưới của tổ chức (TA0008).

Các máy chủ nội bộ

ASD's ACSC đã tiến hành điều tra trên một lượng dữ liệu hạn chế từ phân đoạn hệ thống mạng lưới nội bộ của tổ chức. Các hoạt động độc hại đã được biết đến, dù là họ đã tìm cách hay thành công đều gây ảnh hưởng đến phân đoạn hệ thống mạng lưới nội bộ của tổ chức, bao gồm tác nhân truy cập vào các dữ liệu liên quan đến VDI, thu thập dữ liệu từ máy chủ SQL nội bộ (T1505.001), và lưu lượng mạng bất thường được quan sát thấy từ các địa chỉ IP độc hại đã biết thông qua các thiết bị cổng truy cập (TA0011).

Sử dụng quyền truy cập vào thiết bị bị xâm nhập, nhóm này đã thu thập các tên người sử dụng hợp lệ, mật mã (T1003), và các giá trị mã thông báo xác thực đa yếu tố (MFA token) (T1111). Nhóm này cũng thu thập các JSON Web Tokens (JWTs) (T1528), một dạng dữ liệu xác thực được sử dụng để tạo các phiên đăng nhập máy tính ảo để bàn. Tác nhân có thể đã sử dụng các thông tin này để tạo ra hoặc

chiếm quyền điều khiển các phiên máy tính ảo để bàn (T1563.002) và truy cập vào phân đoạn hệ thống mạng lưới nội bộ của tổ chức như một người sử dụng hợp pháp (T1078).

Tác nhân cũng đã sử dụng quyền truy cập vào thiết bị bị xâm nhập để thu thập dữ liệu từ máy chủ SQL (T1505.001) nằm trong mạng nội bộ của tổ chức. Tác nhân cũng có thể đã truy cập được dữ liệu này.

Bằng chứng từ cổng truy cập của máy chủ cho thấy có lưu lượng mạng đi qua hoặc đến thiết bị này từ các địa chỉ IP độc hại đã biết. Như đã mô tả ở trên, điều này cũng có nghĩa rằng các tác nhân mạng đã gây ảnh hưởng đến hoặc lợi dụng thiết bị này, có thể để chuyển hướng tấn công vào hệ thống mạng lưới nội bộ.

Dòng thời gian điều tra

Danh sách dưới đây cung cấp một dòng thời gian về các hoạt động chính được phát hiện trong quá trình điều tra.

Thời gian	Sự kiện
Tháng 4 năm 2022	Các địa chỉ IP độc hại đã biết, tương tác với cổng truy cập của máy chủ HOST7. Chưa xác định được mục đích của các tương tác này.
Tháng 4 năm 2022	Tất cả các máy chủ, HOST1, HOST2 và HOST3, đều bị xâm nhập bởi một hoặc nhiều tác nhân, và các web shell đã được cài đặt trên các máy chủ này. Một tập hồ sơ nhật ký ghi chép đã được tạo ra hoặc sửa đổi trên HOST2. Tập hồ sơ này chứa thông tin xác thực có thể đã bị tác nhân thu thập. Các tập hồ sơ /etc/security/opasswd và /etc/shadow đã bị chỉnh sửa trên HOST1 và HOST3, cho thấy rằng các mật mã đã bị thay đổi. Bằng chứng trên HOST1 cho thấy mật mã của người sử dụng 'sshuser' đã bị thay đổi.
Tháng 4 năm 2022	HOST2 đã bị tổ chức tắt. Các web shell bổ sung (T1505.003) đã được tạo ra trên HOST1 và HOST3. HOST1 đã chịu các cuộc tấn công brute force (là phương pháp thử tất cả các kết hợp cho đến khi tìm ra giá trị đúng – brute force) qua SSH từ HOST3. Một tập hồ sơ nhật ký ghi chép đã bị chỉnh sửa (T1070) trên HOST3. Tập hồ sơ này chứa thông tin xác thực (T1078) có thể đã bị tác nhân thu thập. Các JWT bị thu thập (T1528) và được xuất ra tập hồ sơ trên HOST3. HOST3 sau đó đã bị tổ chức tắt. Mọi hoạt động sau thời điểm này đều diễn ra trên HOST1.
Tháng 4 năm 2022	Các web shell bổ sung đã được tạo ra trên HOST1 (T1505.003). Các JWT đã được thu thập và xuất ra một tập hồ sơ trên HOST1.
Tháng 4 năm 2022	Các web shell bổ sung đã được tạo ra trên HOST1 (T1505.003), và một địa chỉ IP độc hại đã biết, đã tương tác với máy chủ này (TA0011). Một địa chỉ IP độc hại đã biết, cũng đã tương tác với cổng truy cập của máy chủ HOST7.
Tháng 5 năm 2022	Một địa chỉ IP độc hại đã biết đã tương tác với cổng truy cập của máy chủ HOST7 (TA0011). Một sự kiện xác thực cho một người sử dụng có liên quan đến địa chỉ IP độc hại đã biết được ghi nhận trong nhật ký ghi chép trên HOST1. Một web shell bổ sung cũng được tạo trên máy chủ này (T1505.003).
Tháng 5 năm 2022	Một tập lệnh trên HOST1 đã bị một tác nhân chỉnh sửa (T1543). Tập lệnh này chứa chức năng có thể được sử dụng để thu thập dữ liệu từ một máy chủ SQL nội bộ.
Tháng 5 năm 2022	Một tập hồ sơ nhật ký ghi chép bổ sung trên HOST1 đã được chỉnh sửa lần cuối (T1070). Tập hồ sơ này chứa các cặp tên người sử dụng và mật mã thuộc hệ thống mạng lưới của tổ chức, và được cho là hợp lệ (T1078).
Tháng 5 năm 2022	Một tập hồ sơ ghi chép nhật ký bổ sung đã được chỉnh sửa lần cuối (T1070). Tập hồ sơ này chứa các JWT thu thập được từ HOST1.
Tháng 5 năm 2022	Các web shell bổ sung được tạo ra trên HOST1 (T1505.003). Vào ngày này, tổ chức đã trình báo với Trung tâm An ninh Mạng Úc trực thuộc Tổng cục Tín hiệu Úc (ASD's ACSC) về việc phát hiện một web shell có ngày tạo ra là tháng 4 năm 2022.
Tháng 5 năm 2022	Một số tập lệnh được tạo ra trên HOST1, bao gồm một tập lệnh mang tên Log4jHotPatch.jar.
Tháng 5 năm 2022	Lệnh iptables-save được sử dụng để cho thêm hai cổng mở vào cổng truy cập của máy chủ. Các cổng là 9998 và 9999 (T1572).

Chiến thuật và kỹ thuật của tác nhân

Dưới đây là một số chiến thuật và kỹ thuật được xác định trong quá trình điều tra.

Quyền Truy cập Ban đầu

T1190 Khai thác Ứng dụng có kết nối công khai

Nhóm này có thể đã khai thác các lỗ hổng RCE, đặc quyền nâng cao, và vượt qua xác thực trong sản phẩm quản lý danh tính và đăng nhập truy cập từ xa, để có được quyền truy cập ban đầu vào hệ thống mạng lưới.

Phương thức truy cập ban đầu này được xem là khả thi nhất dựa trên các yếu tố sau: :

- Máy chủ dễ bị tấn công bởi các lỗ hổng CVE này vào thời điểm đó;
- Có các nỗ lực khai thác các lỗ hổng này từ hạ tầng cơ sở của tác nhân đã biết; và
- Hoạt động độc hại nội bộ đầu tiên được ghi nhận xảy ra ngay sau các nỗ lực khai thác vừa diễn ra.

Thực hiện

T1059.004 Trình Thông dịch Lệnh và Tập lệnh: Unix Shell

Nhóm này đã thành công trong việc khai thác các lỗ hổng nêu trên, và có thể đã chạy các lệnh trong Unix shell có sẵn trên thiết bị bị ảnh hưởng. Không có thông tin với đầy đủ chi tiết về các lệnh do tác nhân chạy vì không được thiết bị ghi chép lại.

Duy trì truy cập

T1505.003 Thành phần Phần Mềm Máy Chủ: Web Shell

Các tác nhân đã triển khai nhiều web shell trên thiết bị bị ảnh hưởng. Có thể nhiều tác nhân riêng biệt đã triển khai web shell, nhưng chỉ một số ít tác nhân đã sử dụng các web shell này để thực hiện hoạt động. Web shell cho phép tác nhân thực hiện lệnh tùy ý trên các thiết bị bị xâm nhập.

Chiếm đặc quyền nâng cao trong hệ thống

T1068 Khai thác để chiếm Đặc quyền Nâng cao

Bằng chứng hiện có không giải thích rõ mức độ đặc quyền mà các tác nhân đã đạt được. Tuy nhiên, với việc sử dụng web shell, các tác nhân có thể đã đạt được mức đặc quyền tương đương với đặc quyền của máy chủ mạng trên thiết bị bị xâm nhập. Các lỗ hổng được cho là tồn tại trên thiết bị bị xâm nhập có thể đã cho phép các tác nhân đạt được đặc quyền root (là đặc quyền truy cập cao nhất trên một hệ thống máy tính hoặc hệ thống mạng lưới – Root).

Quyền Truy cập Thông tin Xác thực

T1056.003 Thu thập Dữ liệu Đầu vào: Thu thập Dữ liệu từ Cổng Thông tin Mạng

Bằng chứng trên thiết bị bị xâm nhập cho thấy tác nhân đã thu thập được vài trăm cặp tên người sử dụng và mật mã, dưới dạng chữ viết rõ ràng, và được cho là hợp lệ. Có thể những thông tin này được thu thập bằng cách chỉnh sửa quy trình xác thực chính thức để xuất thông tin đăng nhập ra một tập hồ sơ.

T1111 Chặn Bắt Xác thực Đa Yếu tố (Multi-Factor Authentication Interception)

Tác nhân cũng đã thu thập giá trị của các mã thông báo MFA tương ứng với các lần đăng nhập hợp lệ. Có thể những giá trị này được thu thập bằng cách chỉnh sửa quy trình xác thực chính thức để xuất các giá trị này ra tập hồ sơ. Không có bằng chứng cho thấy "máy chủ bí mật" lưu trữ các giá trị độc nhất để bảo vệ tính an toàn của mã thông báo MFA bị xâm phạm.

T1040 Nghe Lén Hệ thống mạng lưới (Network Sniffing)

Tác nhân được cho là đã lấy được JWT bằng cách chặn bắt lưu lượng HTTP trên thiết bị bị xâm phạm. Có bằng chứng cho thấy tiện ích tcpdump (utility tcpdump) đã được thực hiện trên thiết bị bị xâm nhập, đây có thể là cách tác nhân thu thập các JWTs.

T1539 Đánh cắp Cookie của Phiên Mạng

Như đã mô tả ở trên, tác nhân đã thu thập JWTs, tương tự như cookie phiên mạng. Tác nhân có thể đã tái sử dụng những JWT này để thành lập quyền truy cập tiếp theo.

Khám phá

T1046 Khám phá Dịch vụ của Hệ thống mạng lưới

Có bằng chứng cho thấy tiện ích quét mạng 'nmap' đã được thực hiện trên thiết bị bị xâm nhập để quét các thiết bị khác trong cùng phân đoạn của hệ thống mạng lưới. Có thể tác nhân đã sử dụng công cụ này để khám phá các dịch vụ của hệ thống mạng lưới khả dụng khác, tạo cơ hội cho việc di chuyển hàng ngang trong mạng.

Thu thập dữ liệu

Bằng chứng hiện có không giải thích được cách thức các tác nhân thu thập dữ liệu, hoặc chính xác những gì đã bị lấy đi từ thiết bị bị xâm phạm hoặc từ các hệ thống khác. Tuy nhiên, rất có thể các tác nhân đã truy cập được tất cả các tập hồ sơ trên thiết bị bị xâm nhập, bao gồm cả thông tin đăng nhập bị thu thập (T1003), giá trị mã thông báo MFA (T1111) và các JWT đã mô tả ở trên.

Chỉ huy và Điều khiển

T1071.001 Giao thức Tầng lớp Ứng dụng: Giao thức Mạng

Các tác nhân đã sử dụng web shell để điều khiển và kiểm soát. Các lệnh web shell có thể được truyền qua giao thức HTTPS sử dụng máy chủ mạng hiện có trên thiết bị (T1572).

T1001.003 Làm Mờ Dữ liệu: Mạo danh Giao thức

Các tác nhân đã sử dụng các thiết bị bị xâm nhập làm điểm xuất phát cho các cuộc tấn công được thiết kế để hòa lẫn chung với lưu lượng hợp pháp.

Khuyến cáo về việc phát hiện và biện pháp giảm thiểu rủi ro

Trung tâm An ninh Mạng Úc trực thuộc Tổng cục Tín hiệu Úc (ASD's ACSC) khuyến cáo mạnh mẽ việc triển khai Tám Chiến lược Giảm thiểu Thiết yếu (Essential Eight) của Tổng cục Tín hiệu Úc và các biện pháp Kiểm soát liên quan nhằm Giảm thiểu các Vấn đề An ninh Mạng. Dưới đây là các khuyến cáo về các thực hành bảo mật mạng cần thực hiện để phát hiện và ngăn chặn các cuộc xâm nhập của APT40, kèm theo các biện pháp giảm thiểu rủi ro cụ thể cho bốn TTP chính được tóm tắt trong Bảng 1.

Phát hiện

Một số tập hồ sơ được xác định ở trên đã bị đặt vào các vị trí như C:\Users\Public* và C:\Windows\Temp*. Các vị trí này thường là nơi thuận tiện để ghi chép dữ liệu vì chúng thường cho phép tất cả người sử dụng (đề cập đến việc bất kỳ người sử dụng nào trên hệ thống cũng có thể sửa đổi - world writable) có quyền truy cập, nghĩa là tất cả các tài khoản của người sử dụng đăng ký trên Windows đều có thể truy cập thư mục này và các thư mục con của nó. Thường thì bất kỳ người sử dụng nào cũng có thể truy cập các tập hồ sơ này, điều này tạo điều kiện cho việc di chuyển hàng ngang, né tránh phòng thủ, thực hiện với đặc quyền thấp, và chuẩn bị cho việc đánh cắp dữ liệu.

Các quy tắc Sigma dưới đây tìm kiếm các hoạt động thực hiện từ những vị trí đáng nghi ngờ như một chỉ dấu của hoạt động bất thường. Trong mọi trường hợp, cần tiến hành điều tra thêm để xác nhận hoạt động độc hại và xác định thủ phạm.

Tựa đề: Thực hiện từ Thư mục có Quyền Sửa đổi Trên Toàn Hệ thống - Temp

ID: d2fa2d71-fbd0-4778-9449-e13ca7d7505c

Mô tả: Phát hiện quá trình thực hiện từ C:\Windows\Temp.

Bối cảnh:

Quy tắc này tập trung cụ thể vào việc phát hiện các hoạt động thực hiện xuất phát từ thư mục C:\Windows\Temp*. Thư mục Temp được sử dụng rộng rãi hơn bởi các ứng dụng lành tính, và do đó là dấu vết độc hại có độ tin cậy thấp hơn so với việc thực thi ngoài các thư mục con có quyền sửa đổi trên toàn hệ thống khác trong C:\Windows.

Việc loại bỏ các ứng dụng được thực hiện bởi người sử dụng SYSTEM hoặc NETWORK SERVICE sẽ giảm thiểu đáng kể số lượng hoạt động lành tính được quy tắc này chọn ra.

Điều này đồng nghĩa với việc quy tắc có thể bỏ sót các thực hiện độc hại với mức đặc quyền cao hơn, nhưng việc sử dụng các quy tắc khác để xác định xem có ai đó đang cố gắng nâng cấp đặc quyền lên SYSTEM hay không cũng vẫn là điều nên làm.

Điều tra:

1. Kiểm tra thông tin liên quan trực tiếp đến việc thực hiện tập hồ sơ (file execution), như bối cảnh người sử dụng (user context), mức độ toàn vẹn thực hiện (execution integrity level), hoạt động tiếp theo ngay lập tức và các hình ảnh được tập hồ sơ tải.
2. Điều tra các dữ liệu hỗ trợ liên quan đến quy trình, hệ thống mạng lưới, tập hồ sơ và các thông tin khác trên máy chủ để đánh giá xem hoạt động đó có phải là độc hại hay không.
3. Nếu cần, cố gắng thu thập bản sao của tập hồ sơ để thực hiện phân tích ngược (reverse engineering) nhằm xác định tính hợp pháp của nó.

Tài liệu Tham khảo:

https://www.elastic.co/guide/en/security/current/process-execution-from-an-unusual-directory.html

Tác giả: ACSC của ASD

Ngày: 2024/06/19

Trạng thái: thử nghiệm

Thẻ:

- tlp.green
- classification.au.official
- attack.execution

Nguồn Nhật ký Ghi chép:

```
category: process_creation
product: windows
```

Phát hiện:

```
temp:
    Image|startswith: 'C:\\Windows\\Temp\\'
common_temp_path:
    Image|re|ignorecase: 'C:\\Windows\\Temp\\\
    {[a-fA-F0-9]{8}-([a-fA-F0-9]{4}-){3}[a-fA-F0-9]
    {12}\}\\'
system_user:
    User:
    - 'SYSTEM'
    - 'NETWORK SERVICE'
```

dismhost:

Image|endswith: 'dismhost.exe'

known_parent:

ParentImage|endswith:

- '\\esif_uf.exe'
- '\\vmtoolsd.exe'
- '\\cwainstaller.exe'
- '\\trolleyexpress.exe'

điều kiện: tạm thời và không (common_temp_path or system_user or dismhost or known_parent)

Cảnh báo sai:

- Các ứng dụng kiểm toán nằm trong danh sách cho phép (allowlist) đã được phát hiện thấy chạy các tập hồ sơ thực hiện từ thư mục Temp.
- Thư mục Temp hợp pháp có thể chứa nhiều ứng dụng cài đặt và lập trình khởi chạy, nên cần xem xét mức độ phổ biến của hành vi này trên hệ thống mạng lưới được giám sát (và liệu có nên đưa vào danh sách cho phép hay không) trước khi triển khai quy tắc này.

Mức độ: thấp

Tựa đề: Thực hiện có Quyền Sửa đổi Toàn diện - Không phải- Thư mục Con Hệ thống Tạm thời

ID: 5b187157-e892-4fc9-84fc-aa48aff9f997

Mô tả: Phát hiện tiến trình thực hiện từ vị trí có quyền sửa đổi trên toàn hệ thống trong thư mục con của vị trí cài đặt hệ điều hành (OS) Windows.

Bối cảnh:

Quy tắc này tập trung cụ thể vào việc phát hiện thực thi từ các thư mục có quyền trên toàn hệ thống trong ổ đĩa C:\, đặc biệt là trong C:\Windows*, ngoại trừ C:\Windows\Temp (vì thư mục này thường được sử dụng bởi các ứng dụng hợp lệ, do đó là một chỉ dấu độc hại có độ tin cậy thấp hơn).

Các thư mục AppData sẽ bị loại trừ nếu tập hồ sơ được chạy dưới dạng SYSTEM - đây là một cách thức vô hại mà nhiều tập hồ sơ ứng dụng tạm thời được thực hiện.

Sau khi hoàn tất việc tạo ra tiêu chuẩn (baseline) hệ thống mạng lưới ban đầu, và xác định các hoạt động thực hiện vô hại từ các vị trí này, quy tắc này sẽ hiếm khi được khởi động.

Điều tra:

1. Kiểm tra thông tin liên quan trực tiếp đến việc thực hiện tập hồ sơ này, chẳng hạn như ngữ cảnh người sử dụng, mức độ toàn vẹn thực hiện, các hoạt động tiếp theo ngay lập tức, và các hình ảnh được tập hồ sơ tải.
2. Điều tra các dữ liệu ngữ cảnh liên quan đến tiến trình, hệ thống mạng lưới, tập hồ sơ và các dữ liệu hỗ trợ khác trên máy chủ để giúp đánh giá xem hoạt động có phải là độc hại hay không.
3. Nếu cần thiết, cố gắng thu thập một bản sao của tập hồ sơ để phân tích ngược (reverse engineering) nhằm xác định tính hợp pháp của tập hồ sơ.

Tài liệu tham khảo:

https://gist.github.com/mattifestation/5f9de750470c9e0e1f9c9c33f0ec3e56

https://www.elastic.co/guide/en/security/current/process-execution-from-an-unusual-directory.html

Tác giả: Trung tâm An ninh Mạng Úc trực thuộc Tổng cục Tín hiệu Úc (ASD's ACSC)

Ngày: 2024-06-19
Trạng thái: thử nghiệm

Tags:

- tlp.green
- classification.au.official
- attack.execution

Nguồn Nhật ký Ghi chép:

category: process_creation
product: windows

Phát hiện:

writable_path:

Image|contains:

- ':\\$Recycle.Bin\\'
- ':\\AMD\\Temp\\'
- ':\\Intel\\'
- ':\\PerfLogs\\'
- ':\\Windows\\addins\\'
- ':\\Windows\\appcompat\\'
- ':\\Windows\\apppatch\\'
- ':\\Windows\\AppReadiness\\'
- ':\\Windows\\bcastdvr\\'
- ':\\Windows\\Boot\\'
- ':\\Windows\\Branding\\'
- ':\\Windows\\CbsTemp\\'
- ':\\Windows\\Containers\\'
- ':\\Windows\\csc\\'
- ':\\Windows\\Cursors\\'
- ':\\Windows\\debug\\'
- ':\\Windows\\diagnostics\\'
- ':\\Windows\\DigitalLocker\\'
- ':\\Windows\\dot3svc\\'
- ':\\Windows\\en-US\\'
- ':\\Windows\\Fonts\\'
- ':\\Windows\\Globalization\\'
- ':\\Windows\\Help\\'
- ':\\Windows\\IdentityCRL\\'
- ':\\Windows\\IME\\'
- ':\\Windows\\ImmersiveControlPanel\\'
- ':\\Windows\\INF\\'
- ':\\Windows\\intel\\'

- ':\\Windows\\L2Schemas\\'
- ':\\Windows\\LiveKernelReports\\'
- ':\\Windows\\Logs\\'
- ':\\Windows\\media\\'
- ':\\Windows\\Migration\\'
- ':\\Windows\\ModemLogs\\'
- ':\\Windows\\ms\\'
- ':\\Windows\\OCR\\'
- ':\\Windows\\panther\\'
- ':\\Windows\\Performance\\'
- ':\\Windows\\PLA\\'
- ':\\Windows\\PolicyDefinitions\\'
- ':\\Windows\\Prefetch\\'
- ':\\Windows\\PrintDialog\\'
- ':\\Windows\\Provisioning\\'
- ':\\Windows\\Registration\\CRMLog\\'
- ':\\Windows\\RemotePackages\\'
- ':\\Windows\\rescache\\'
- ':\\Windows\\Resources\\'
- ':\\Windows\\SchCache\\'
- ':\\Windows\\schemas\\'
- ':\\Windows\\security\\'
- ':\\Windows\\ServiceState\\'
- ':\\Windows\\servicing\\'
- ':\\Windows\\Setup\\'
- ':\\Windows\\ShellComponents\\'
- ':\\Windows\\ShellExperiences\\'
- ':\\Windows\\SKB\\'
- ':\\Windows\\TAPI\\'
- ':\\Windows\\Tasks\\'
- ':\\Windows\\TextInput\\'
- ':\\Windows\\tracing\\'
- ':\\Windows\\Vss\\'
- ':\\Windows\\WaaS\\'
- ':\\Windows\\Web\\'
- ':\\Windows\\wlansvc\\'
- ':\\Windows\\System32\\Com\\dmp\\'
- ':\\Windows\\System32\\FxsTmp\\'
- ':\\Windows\\System32\\Microsoft\\Crypto\\RSA\\MachineKeys\\'
- ':\\Windows\\System32\\Speech\\'
- ':\\Windows\\System32\\spool\\drivers\\color\\'
- ':\\Windows\\System32\\spool\\PRINTERS\\'
- ':\\Windows\\System32\\spool\\SERVERS\\'
- ':\\Windows\\System32\\Tasks_Migrated\\Microsoft\\Windows\\PLA\\System\\'
- ':\\Windows\\System32\\Tasks\\'
- ':\\Windows\\SysWOW64\\Com\\dmp\\'
- ':\\Windows\\SysWOW64\\FxsTmp\\'
- ':\\Windows\\SysWOW64\\Tasks\\'

appdata:

Image|contains: '\\AppData\\'
Người Sử dụng: 'HỆ THỐNG'

điều kiện: writable_path và không phải appdata

Cảnh báo sai:

Các ứng dụng kiểm toán trong danh sách cho phép đã được phát hiện thấy chạy các tập hồ sơ thực hiện từ những thư mục này.

Có thể các tập lệnh và công cụ quản trị được sử dụng trong môi trường được giám sát nằm trong một trong những thư mục này và cần được giải quyết theo từng trường hợp cụ thể.

Mức độ: cao

Tựa đề: Thực thi có Quyền Sửa đổi Toàn diện - Người Sử dụng

ID 6dda3843-182a-4214-9263-925a80b4c634

Mô tả: Phát hiện quá trình thực thi từ C:\Users\Public* và các thư mục có quyền sửa đổi toàn diện khác trong Users.

Bối cảnh:

Các thư mục AppData sẽ được loại trừ nếu tập hồ sơ được chạy dưới quyền SYSTEM - đây là cách hợp pháp mà nhiều tập hồ sơ ứng dụng tạm thời được thực thi.

Điều tra:

1. Kiểm tra thông tin liên quan trực tiếp đến việc thực hiện tập hồ sơ, chẳng hạn như ngữ cảnh người dùng, mức độ toàn vẹn khi thực hiện, các hoạt động tiếp theo ngay lập tức và các hình ảnh được tập hồ sơ tải.
2. Điều tra các tiến trình, hệ thống mạng lưới, tập hồ sơ và dữ liệu hỗ trợ liên quan trên máy chủ để đánh giá hoạt động đó có phải là độc hại hay không.
3. Nếu cần thiết, thu thập bản sao tập hồ sơ để phân tích ngược nhằm xác định tính hợp pháp của tập hồ sơ.

Tài liệu Tham khảo:

https://www.elastic.co/guide/en/security/current/process-execution-from-an-unusual-directory.html

Tác giả: Trung tâm An ninh Mạng Úc trực thuộc Tổng cục Tín hiệu Úc (ASD's ACSC)

Ngày: 2024/06/19

Trạng thái: thử nghiệm

Tags:

- tlp.green
- classification.au.official
- attack.execution

Nguồn Nhật ký Ghi chép:

danh mục: tạo quy trình (process_creation)
sản phẩm: windows

Phát hiện:

người sử dụng:

Image|contains:

- ':\\Users\\All Users\\'
- ':\\Users\\Contacts\\'
- ':\\Users\\Default\\'
- ':\\Users\\Public\\'
- ':\\Users\\Searches\\'

appdata:

Image|contains: '\\AppData\\'
Người sử dụng: 'SYSTEM'

điều kiện: người sử dụng và không phải appdata

Cảnh báo sai:

- Có thể các tập lệnh và công cụ quản trị được sử dụng trong môi trường được giám sát nằm trong thư mục Công khai (Public) hoặc các thư mục con của nó, và cần được giải quyết theo từng trường hợp cụ thể.

Mức độ: trung bình

Biện pháp giảm thiểu rủi ro

Nhật ký Ghi chép

Trong quá trình điều tra của Trung tâm An ninh Mạng Úc trực thuộc Tổng cục Tín hiệu Úc (ASD's ACSC), một vấn đề thường gặp làm giảm hiệu quả và tốc độ của các nỗ lực điều tra là việc thiếu thông tin nhật ký ghi chép toàn diện và trình tự thời gian của các sự kiện trên nhiều lĩnh vực, bao gồm nhật ký ghi chép yêu cầu của máy chủ web, nhật ký ghi chép sự kiện Windows và nhật ký ghi chép:proxy internet.

Trung tâm An ninh Mạng Úc trực thuộc Tổng cục Tín hiệu Úc (ASD's ACSC) khuyến cáo việc xem xét và áp dụng các hướng dẫn của họ về Ghi chép và Chuyển tiếp Sự kiện của Windows, bao gồm các tập hồ sơ cấu hình và tập lệnh trong Kho Lưu trữ Ghi Sự kiện Windows và Hướng dẫn Theo dõi Hệ thống trong Sổ tay An ninh Thông tin, bao gồm việc gom về trung tâm tất cả nhật ký ghi chép và lưu giữ nhật ký ghi chép trong khoảng thời gian phù hợp.

Quản lý bản vá

Nên nhanh chóng vá lỗi cho tất cả các thiết bị và dịch vụ có kết nối với Internet, bao gồm máy chủ mạng, ứng dụng mạng, và các cổng truy cập từ xa. Cân nhắc việc áp dụng hệ thống quản lý bản vá tập trung để tự động hóa và tăng tốc quá trình này. Trung tâm An ninh Mạng Úc trực thuộc Tổng cục Tín hiệu Úc (ASD's ACSC) khuyến cáo thực hiện theo Hướng dẫn Quản lý Hệ thống của ISM, đặc biệt là các kiểm soát Vá Hệ thống những khi có thể áp dụng.

Hầu hết các khai thác mà các tác nhân sử dụng đều là các lỗ hổng đã được công khai và có bản vá, hoặc biện pháp giảm thiểu sẵn có. Các tổ chức nên bảo đảm rằng các bản vá bảo mật hoặc các biện pháp giảm thiểu rủi ro được áp dụng cho hạ tầng cơ sở có kết nối với Internet trong vòng 48 giờ, và nếu có thể, sử dụng các phiên bản phần mềm và hệ điều hành mới nhất.

Phân đoạn hệ thống mạng lưới

Phân đoạn hệ thống mạng lưới có thể làm cho việc đối thủ tìm kiếm và truy cập vào dữ liệu nhạy cảm của tổ chức trở nên khó khăn hơn nhiều. Phân đoạn hệ thống mạng lưới để giới hạn hoặc ngăn chặn việc di chuyển hàng ngang bằng cách từ chối lưu lượng giữa các máy vi tính trừ khi cần thiết. Các máy chủ quan trọng như Active Directory và các máy chủ xác thực khác chỉ nên được điều hành từ một số lượng các máy chủ trung gian hạn chế, hoặc 'máy chủ nhảy' (jump servers). Những máy chủ này cần được giám sát chặt chẽ, bảo mật tốt, và giới hạn người sử dụng, cũng như các thiết bị nào được phép kết nối với nó.

Dù đã có những trường hợp ngăn chặn được sự di chuyển hàng ngang được xác định, việc phân đoạn của hệ thống mạng lưới bổ sung cũng có thể đã giúp hạn chế hơn nữa lượng dữ liệu mà các tác nhân có thể truy cập và đánh cắp.

Các biện pháp giảm thiểu bổ sung

Các cơ quan soạn thảo cũng khuyến cáo các biện pháp giảm thiểu rủi ro sau đây để đối đầu với APT40 và các nhóm khác sử dụng các kỹ thuật, thủ thuật và phương sách (TTPs) dưới đây:

- Vô hiệu hóa các dịch vụ của hệ thống mạng lưới, cổng và giao thức không sử dụng hoặc không cần thiết.
- Sử dụng tường lửa ứng dụng mạng (WAF) được tinh chỉnh tốt để bảo vệ máy chủ mạng và các ứng dụng.
- Thực hiện nguyên tắc ít đặc quyền nhất để giới hạn quyền truy cập vào máy chủ, chia sẻ các tập hồ sơ, và các nguồn lực khác.
- Sử dụng xác thực đa yếu tố (MFA) và tài khoản dịch vụ được quản lý để làm cho thông tin đăng nhập khó bị xâm phạm và tái sử dụng hơn. MFA nên được áp dụng cho tất cả các dịch vụ truy cập từ xa qua internet, bao gồm:
  - Email mạng và email dựa trên đám mây
  - Các nền tảng cộng tác
  - Kết nối hệ thống mạng lưới ảo riêng (VPN)
  - Dịch vụ máy vi tính để bàn từ xa
- Thay thế thiết bị đã hết hạn sử dụng.

Bảng 1. Chiến lược/Kỹ thuật Giảm thiểu Rủi ro

TTP	Tám Chiến lược Giảm thiểu Thiết yếu	Kiểm soát ISM
Quyền Truy cập Ban đầu T1190 Khai thác Ứng dụng Công khai	Cập nhật bản vá cho ứng dụng Cập nhật bản vá cho hệ điều hành Xác thực Đa Yếu tố Kiểm soát ứng dụng	ISM-0140 ISM-1698 ISM-1701 ISM-1921 ISM-1876 ISM-1877 ISM-1905
Thực hiện T1059 Trình thông dịch lệnh và tập lệnh	Kiểm soát ứng dụng Hạn chế macro trong Microsoft Office Hạn chế đặc quyền quản trị	ISM-0140 ISM-1490 ISM-1622 ISM-1623 ISM-1657 ISM-1890
Duy trì Truy cập T1505.003 Thành phần Phần mềm Máy Chủ: Web Shell	Kiểm soát Ứng dụng Hạn chế đặc quyền quản trị	ISM-0140 ISM-1246 ISM-1746 ISM-1249 ISM-1250 ISM-1490 ISM-1657 ISM-1871
Truy cập ban đầu / Chiếm Đặc quyền Nâng cao trong Hệ thống / Duy trì Truy cập T1078 Tài khoản Hợp lệ	Cập nhật hệ điều hành Xác thực Đa Yếu tố Giới hạn quyền quản trị Kiểm soát ứng dụng Tăng cường ứng dụng người sử dụng	ISM-0140 ISM-0859 ISM-1546 ISM-1504 ISM-1679

Để biết thêm các khuyến cáo chung về việc phát hiện và giảm thiểu rủi ro, xin vui lòng tham khảo các mục Giảm thiểu Rủi ro và Phát hiện trong phần kỹ thuật trên trang mạng kỹ thuật MITRE ATT&CK cho từng kỹ thuật được xác định trong phần tóm tắt về MITRE ATT&CK ở cuối tài liệu khuyến cáo này.

Tuyên bố miễn trừ trách nhiệm

Thông tin trong phúc trình này được cung cấp "nguyên trạng" chỉ nhằm mục đích cung cấp thông tin mà thôi. Các cơ quan soạn thảo không xác nhận bất kỳ tổ chức thương mại, sản phẩm, công ty, hoặc dịch vụ nào, bao gồm cả các tổ chức, sản phẩm, hoặc dịch vụ được đề cập đến trong tài liệu này. Bất kỳ việc đề cập nào đến các tổ chức thương mại, sản phẩm, phương sách, hoặc dịch vụ cụ thể dưới dạng nhãn hiệu dịch vụ, nhãn hiệu thương mại, nhà sản xuất, hoặc hình thức khác, đều không đại diện hoặc ngụ ý sự xác nhận, khuyến nghị, hoặc thiên vị từ phía các cơ quan soạn thảo.

Tài liệu này được đánh dấu TLP:CLEAR. Việc tiết lộ không bị hạn chế. Các nguồn có thể sử dụng TLP:CLEAR khi thông tin mang ít hoặc không có nguy cơ bị sử dụng sai mục đích có thể dự đoán, theo đúng các quy tắc và thủ tục hiện hành về việc công bố công khai. Theo các quy định tiêu chuẩn về bản quyền, thông tin TLP:CLEAR có thể được phân phối không giới hạn. Để biết thêm thông tin về Giao thức Đèn Giao Thông (Traffic Light Protocol), hãy xem cisa.gov/tlp.

MITRE ATT&CK – Kỹ thuật hoạt động đáng chú ý trong quá khứ của nhóm APT40

Dò thám (TA0043)	
Tìm kiếm trên các Trang Mạng Thuộc Sở hữu của Nạn nhân (T1594)	Thu thập Thông tin Nhận Dạng của Nạn nhân: Thông tin đăng nhập (T1589.001)
Quét Chủ động: Quét Lỗ hổng (T1595.002)	Thu thập Thông tin Máy Chủ của Nạn nhân (T1592)
Tìm kiếm Trang mạng mở Rộng /Tên Miền mở Rộng: Công cụ Tìm kiếm (T1593.002)	Thu thập Thông tin Hệ thống mạng lưới của Nạn nhân: Thuộc tính của Tên miền (T1590.001)
Thu thập Thông tin Nhận Dạng của Nạn nhân: Địa chỉ Email (T1589.002)	

Phát triển Nguồn lực (TA0042)	
Mua sắm Hạ tầng Cơ sở: Tên Miền (T1583.001)	Mua sắm Hạ tầng Cơ sở (T1583)
Mua sắm Hạ tầng Cơ sở Máy chủ DNS (T1583.002)	Xâm nhập Tài khoản (T1586)
Phát triển Năng lực: Chứng chỉ Ký Mã (T1587.002)	Xâm nhập Hạ tầng Cơ sở (T1584)
Phát triển Năng lực: Chứng chỉ Kỹ thuật Số (T1587.003)	Phát triển Năng lực: Phần mềm Độc hại (T1587.001)
Thu thập Khả năng: Chứng chỉ Ký Mã (T1588.003)	Tạo Tài khoản: Tài khoản Đám mây (T1585.003)
Xâm phạm Hạ tầng Cơ sở: Thiết bị Mạng (T1584.008)	Thu thập Khả năng: Chứng chỉ Kỹ thuật Số (T1588.004)

Truy cập Ban đầu (TA0001)	
Tài khoản Hợp lệ (T1078)	Lừa đảo (T1566)
Tài khoản Hợp lệ: Tài khoản Mặc định (T1078.001)	Lừa đảo: Tập hồ sơ Đính kèm Lừa đảo Trực tuyến (T1566.001)
Tài khoản Hợp lệ: Tài khoản Miền (T1078.002)	Lừa đảo: Đường dẫn Spearphishing (T1566.002)
Dịch vụ Từ Xa Bên Ngoài (T1133)	Khai thác Ứng dụng Công khai (T1190)
Xâm phạm bằng Kỹ thuật Drive-by (T1189)	

Thực hiện(TA0002)	
Công cụ Quản lý Windows (T1047)	Trình Thông dịch Lệnh và Tập lệnh: Python (T1059.006)
Công việc/Nhiệm vụ được Lên lịch: Tại (T1053.002)	Trình Thông dịch Lệnh và Tập lệnh: JavaScript (T1059.007)
Công việc/Nhiệm vụ được Lên lịch: Công việc được Lên lịch (T1053.005)	API Gốc (T1106)
Trình Thông dịch Lệnh và Tập lệnh (T1059)	Giao tiếp Liên Tiến trình (T1559)
Trình Thông dịch Lệnh và Tập lệnh: Trình Dòng lệnh Windows (T1059.003)	Dịch vụ Hệ thống: Thực hiện Dịch vụ (T1569.002)
Trình Thông dịch Lệnh và Tập lệnh: PowerShell (T1059.001)	Khai thác để Thực hiện trên Máy khách (T1203)
Trình Thông dịch Lệnh và Tập lệnh: Visual Basic (T1059.005)	Thực hiện bởi Người Sử dụng: Tập Hồ sơ Độc hại (T1204.002)
Trình Thông dịch Lệnh và Tập lệnh: Unix Shell (T1059.004)	Trình Thông dịch Lệnh và Tập lệnh: Apple Script (T1059.002)
Công việc/Nhiệm vụ được Lên lịch: Cron (T1053.003)	Công cụ Triển khai Phần mềm (T1072)

Persistence (TA0003)	
Tài khoản Hợp lệ (T1078)	Thành phần Phần mềm Máy Chủ: Web Shell (T1505.003)
Khởi động Ứng dụng Office: Macro Mẫu Office (T1137.001)	Tạo hoặc Sửa đổi Quy trình Hệ thống: Dịch vụ của Windows (T1543.003)
Công việc/Nhiệm vụ được Lên lịch: Tại (T1053.002)	Thực hiện Tự động Khởi động hoặc Đăng nhập: Khóa Chạy Registry (cơ sở dữ liệu phân cấp – Registry)/Thư mục Khởi động (T1547.001)
Công việc/Nhiệm vụ được Lên lịch: Công việc được Lên lịch (T1053.005)	Thực hiện Khởi động hoặc Đăng nhập Tự động: Sửa đổi Phím Tắt (shortcut) (T1547.009)
Dịch vụ Từ xa Bên ngoài (T1133)	Luồng Thực hiện Hijack (tấn công chiếm quyền điều khiển): Lệnh Lừa đảo Tìm kiếm DLL (T1574.001)
Công việc/Nhiệm vụ được Lên lịch: Cron (T1053.003)	Luồng Thực hiện Hijack (tấn công chiếm quyền điều khiển): Tấn công Thứ tự Tải DLL (T1574.002)
Thao túng Tài khoản (T1098)	Tài khoản Hợp lệ: Tài khoản Đám mây (T1078.004)
Tài khoản Hợp lệ: Tài khoản Miền (T1078.002)	

Chiếm Đặc quyền Nâng cao trong Hệ thống (TA0004)	
Công việc/Nhiệm vụ được Lên lịch: Tại (T1053.002)	Tạo hoặc Sửa đổi Quy trình của Hệ thống: Dịch vụ Windows (T1543.003)
Công việc/Nhiệm vụ được Lên lịch: Công việc được Lên lịch (T1053.005)	Thực hiện Khởi động hoặc Đăng nhập Tự động: Khóa Chạy Registry (cơ sở dữ liệu phân cấp – Registry)/Thư mục Khởi động (T1547.001)
Quá trình Tiêm vào: Chiếm quyền Thực hiện Luồng (T1055.003)	Thực hiện Khởi động hoặc Đăng nhập Tự động: Sửa đổi Phím tắt (T1547.009)
Quá trình Tiêm vào: Quá trình Làm Rỗng (T1055.012)	Luồng Thực hiện Hijack (tấn công chiếm quyền điều khiển): Chiếm quyền Thứ tự Tìm kiếm DLL (T1574.001)

Chiếm Đặc quyền Nâng cao trong Hệ thống (TA0004)	
Tài khoản hợp lệ: Tài khoản Miền (T1078.002)	Khai thác để Chiếm Đặc quyền Nâng cao trong Hệ thống (T1068)
Thao túng Mã Thông báo Truy cập: Mạo danh/Ăn cắp Mã Thông báo (T1134.001)	Thực hiện Kích hoạt Sự kiện: Sửa đổi Cấu hình Unix Shell (T1546.004)
Quá trình Tiêm vào: Tiêm vào (DDL) Thư viện Liên kết Động (T1055.001)	Tài khoản hợp lệ: Tài khoản Miền (T1078.002)
Tài khoản Hợp lệ: Tài khoản Cục bộ (T1078.003)	

Né tránh Phòng thủ (TA0005)	
Rootkit (T1014)	Thực hiện Lệnh Gián tiếp (T1202)
Làm rối Tập hồ sơ hoặc Thông tin (T1027)	Thực hiện Proxy Nhị phân Hệ thống: Mshta (T1218.005)
Làm rối Tập hồ sơ hoặc Thông tin: Đóng gói Phần mềm (T1027.002)	Thực hiện Proxy Nhị phân Hệ thống: Regsvr32 (T1218.010)
Làm rối Tập hồ sơ hoặc Thông tin: Thuật ẩn Mã (T1027.003)	Làm Xáo trộn các Biện pháp Kiểm soát Tin cậy: Ký mã (T1553.002)
Làm rối Tập hồ sơ hoặc Thông tin: Biên dịch Sau khi Chuyển giao (T1027.004)	Sửa đổi Quyền Truy cập Tập Hồ sơ và Thư mục: Sửa đổi Quyền Truy cập Tập Hồ sơ Linux và Mac và Thư mục: (T1222.002)
Ngụy trang: So khớp Tên hoặc Vị trí Hợp lệ (T1036.005)	Ảo hóa/Né tránh Sandbox: Kiểm tra Hệ thống (T1497.001)
Quá trình Tiêm vào: Chiếm Quyền Thực hiện Luồng (T1055.003)	Ngụy trang (T1036)
Tải Mã Phản chiếu (T1620)	Làm Suy yếu Phòng thủ: Vô hiệu hóa hoặc Sửa đổi Hệ thống Tường lửa (T1562.004)
Quá trình Tiêm vào: Quá trình Làm rỗng (T1055.012)	Ẩn dấu Hiện vật: Các Tập hồ sơ và Thư mục Ẩn (T1564.001)
Xóa Dấu vết: Xóa Tập Hồ sơ (T1070.004)	Dấu Hiện vật: Window Ẩn (T1564.003)
Xóa Dấu vết: Timestomp (T1070.006)	Luồng Thực hiện Hijack (tấn công chiếm quyền điều khiển): Chiếm Quyền Thứ tự Tìm kiếm DLL (T1574.001)
Xóa Dấu vết: Xóa Nhật ký Ghi chép Sự kiện của Windows (T1070.001)	Luồng Thực hiện Hijack (tấn công chiếm quyền điều khiển): Tấn công Thứ tự Tải DLL (T1574.002)
Sửa đổi Registry (T1112)	Dịch vụ Mạng (T1102)
Gỡ rối/Giải mã tập hồ sơ hoặc thông tin (T1140)	Ngụy trang: Ngụy trang Nhiệm vụ hoặc Dịch vụ (T1036.004)
Làm Suy yếu Phòng thủ (T1562)	

Truy cập Thông tin Xác thực (TA0006)	
Đánh cắp (Dumping) Thông tin Xác thực của Hệ điều hành: Bộ nhớ LSASS (T1003.001)	Thông tin Xác thực Không được Bảo mật: Thông tin Xác thực trong Tập hồ sơ (T1552.001)
Đánh cắp (Dumping) Thông tin Xác thực của Hệ điều hành: NTDS (T1003.003)	Kỹ thuật Brute Force: Đoán Mật mã(T1110.001)
Nghe lén Mạng (T1040)	Xác thực Bắt buộc (T1187)

Truy cập Thông tin Xác thực (TA0006)	
Thông tin Xác thực từ Kho Lưu trữ Mật mã: Móc khóa (T1555.001)	Ăn trộm hoặc Giả mạo Vé Kerberos: Kerberoasting (T1558.003)
Thu thập Dữ liệu Đầu vào: Nhật ký Ghi chép Thao tác Phím (T1056.001)	Ngăn chặn Xác thực Đa yếu tố (T1111)
Ăn trộm Cookie của Phiên Mạng (T1539)	Trộm Mã thông báo Truy cập Ứng dụng (T1528)
Khai thác Truy cập Thông tin Xác thực (T1212)	Kỹ thuật Brute Force: Bẻ khóa Mật mã (T1110.002)
Thu thập Dữ liệu Đầu vào: Thu thập Dữ liệu từ Cổng Thông tin Mạng (T1056.003)	Đánh cắp (Dumping) Thông tin Xác thực của Hệ điều hành DCSync (T1003.006)
Thông tin Đăng nhập từ Kho lưu trữ Mật mã (T1555)	Thông tin Đăng nhập từ Kho lưu trữ Mật mã: Thông tin Đăng nhập từ Trình duyệt Mạng (T1555.003)

Khám phá (TA0007)	
Khám phá Dịch vụ Hệ thống (T1007)	Khám phá Thông tin Hệ thống (T1082)
Khám phá Window Ứng dụng (T1010)	Khám phá Tài khoản: Tài khoản Cục bộ (T1087.001)
Đăng ký Truy vấn (T1012)	Khám phá Thông tin Hệ thống, Kỹ thuật T1082 - Doanh nghiệp | MITRE ATT&CK®
Khám phá Tập hồ sơ và Thư mục (T1083)	Khám phá Thời gian Hệ thống (T1124)
Khám phá Dịch vụ Hệ thống mạng lưới (T1046)	Khám phá Chủ sở hữu/Người sử dụng Hệ thống (T1033)
Khám phá Hệ thống Từ xa (T1018)	Khám phá Độ tin cậy Miền (T1482)
Khám phá Tài khoản: Tài khoản Email (T1087.003)	Khám phá Tài khoản: Tài khoản Miền (T1087.002)
Khám phá Kết nối Hệ thống mạng lưới (T1049)	Né tránh Ảo hóa/Sandbox: Kiểm tra Hệ thống (T1497.001)
Khám phá Quá trình (T1057)	Khám phá Phần mềm (T1518)
Khám phá Quyền của Nhóm: Nhóm Miền (T1069.002)	Khám phá Chia sẻ Mạng, Kỹ thuật T1135 - Doanh nghiệp | MITRE ATT&CK®
Khám phá Cấu hình của Hệ thống Mạng lưới: Khám phá Kết nối Internet (T1016.001)	

Di chuyển Hàng Ngang (TA0008)	
Dịch vụ Từ xa: Giao thức Máy tính Từ xa (T1021.001)	Dịch vụ Từ xa (T1021)
Dịch vụ Từ xa: Chia sẻ Quản trị SMB/Windows (T1021.002)	Sử dụng Tài liệu Xác thực Thay thế: Chuyển Vé (T1550.003)
Dịch vụ Từ xa: Quản lý Windows Từ xa (T1021.006)	Chuyển Công cụ Hàng Ngang (T1570)

Thu thập dữ liệu (TA0009)	
Dữ liệu từ Hệ thống Cục bộ (T1005)	Lưu trữ Dữ liệu Đã thu thập: Lưu trữ qua Thư viện (T1560.002)
Dữ liệu từ Ổ đĩa Chia sẻ của Hệ thống mạng lưới (T1039)	Thu thập Email: Thu thập Email Từ xa (T1114.002)

Thu thập Dữ liệu (TA0009)	
Thu thập Dữ liệu Đầu vào: Nhật ký Ghi chép Thao tác Phím (T1056.001)	Dữ liệu được Lưu trữ Tạm thời (T1115)
Thu thập tự động (T1119)	Dữ liệu từ Kho Thông tin (T1213)
Thu thập Dữ liệu Đầu vào: Thu thập Dữ liệu từ Cổng Thông tin Mạng (T1056.003)	Dữ liệu được Phân đoạn: Phân đoạn Dữ liệu từ xa (T1074.002)
Dữ liệu được Phân đoạn: Phân đoạn Dữ liệu Cục bộ (T1074.001)	Lưu trữ Dữ liệu đã Thu thập (T1560)
Bộ Sưu tập email (T1114)	

Đánh cắp Dữ liệu (TA0010)	
Đánh cắp Dữ liệu Qua Kênh C2 (T1041)	Đánh cắp Dữ liệu Qua Giao thức Thay thế: Đánh cắp Dữ liệu Qua Giao thức Non-C2 được Mã hóa Bất Đối xứng (T1048.002)
Đánh cắp Dữ liệu Qua Giao thức Thay thế (T1048)	Đánh cắp Dữ liệu Qua Dịch vụ Mạng: Đánh cắp Dữ liệu tới Bộ nhớ Đám mây (T1567.002)

Lệnh và Kiểm soát (TA0011)	
Làm Mờ Dữ liệu: Mạo danh Giao thức (T1001.003)	Dịch vụ Mạng: Bộ Giải mã Điểm chết (T1102.001)
Cổng Thường dùng (T1043)	Dịch vụ Mạng: Giao tiếp Một Chiều (T1102.003)
Giao thức Tầng lớp Ứng dụng: Giao thức Mạng (T1071.001)	Chuyển giao Công cụ Ingress (T1105)
Giao thức Tầng lớp Ứng dụng: Giao thức Truyền tải Tập Hồ sơ (T1071.002)	Proxy: Proxy Nội bộ (T1090.001)
Proxy: Proxy Bên Ngoài (T1090.002)	Cổng Không Chuẩn (T1571)
Proxy: Multi-hop Proxy (T1090.003)	Đường Hầm Giao thức (T1572)
Dịch vụ Mạng: Giao tiếp Hai chiều (T1102.002)	Kênh Được Mã hóa (T1573)
Kênh Được Mã hóa: Mã hóa Bất Đối xứng (T1573.002)	Công cụ Chuyển giao Ingress (T1105)
Proxy, Kỹ thuật T1090 - Doanh nghiệp | MITRE ATT&CK®	

Tác động (TA0040)	
Dừng Dịch vụ (T1489)	Xóa Ổ đĩa (T1561)
Tắt/Khởi động lại Hệ thống (T1529)	Chiếm đoạt Nguồn lực (T1496)

Ghi chú

Tuyên bố miễn trừ trách nhiệm

Tài liệu trong hướng dẫn này mang tính chất tổng quát và không nên được coi là cố vấn pháp lý hoặc dựa vào để được giúp đỡ trong bất kỳ trường hợp cụ thể hoặc tình huống khẩn cấp nào. Đối với bất kỳ vấn đề quan trọng nào, quý vị nên tìm kiếm lời khuyên chuyên môn, độc lập và thích hợp liên quan đến hoàn cảnh của mình.

Chính phủ Liên bang không chịu trách nhiệm hoặc trách nhiệm pháp lý nào đối với bất kỳ thiệt hại, mất mát hoặc chi phí nào phát sinh do việc dựa vào thông tin có trong hướng dẫn này.

Bản quyền

Sử dụng Quốc huy

Các điều khoản về việc sử dụng Quốc huy như được trình bày chi tiết trên trang mạng của Bộ Thủ tướng và Nội các Commonwealth Coat of Arms Information and Guidelines | pmc.gov.au.

Muốn biết thêm thông tin, hoặc muốn trình báo vấn đề an ninh mạng, xin hãy liên lạc với chúng tôi:

cyber.gov.au | 1300 CYBER1 (1300 292 371)

Số điện thoại này chỉ được sử dụng ở trong nước Úc mà thôi.

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian Cyber Security Centre