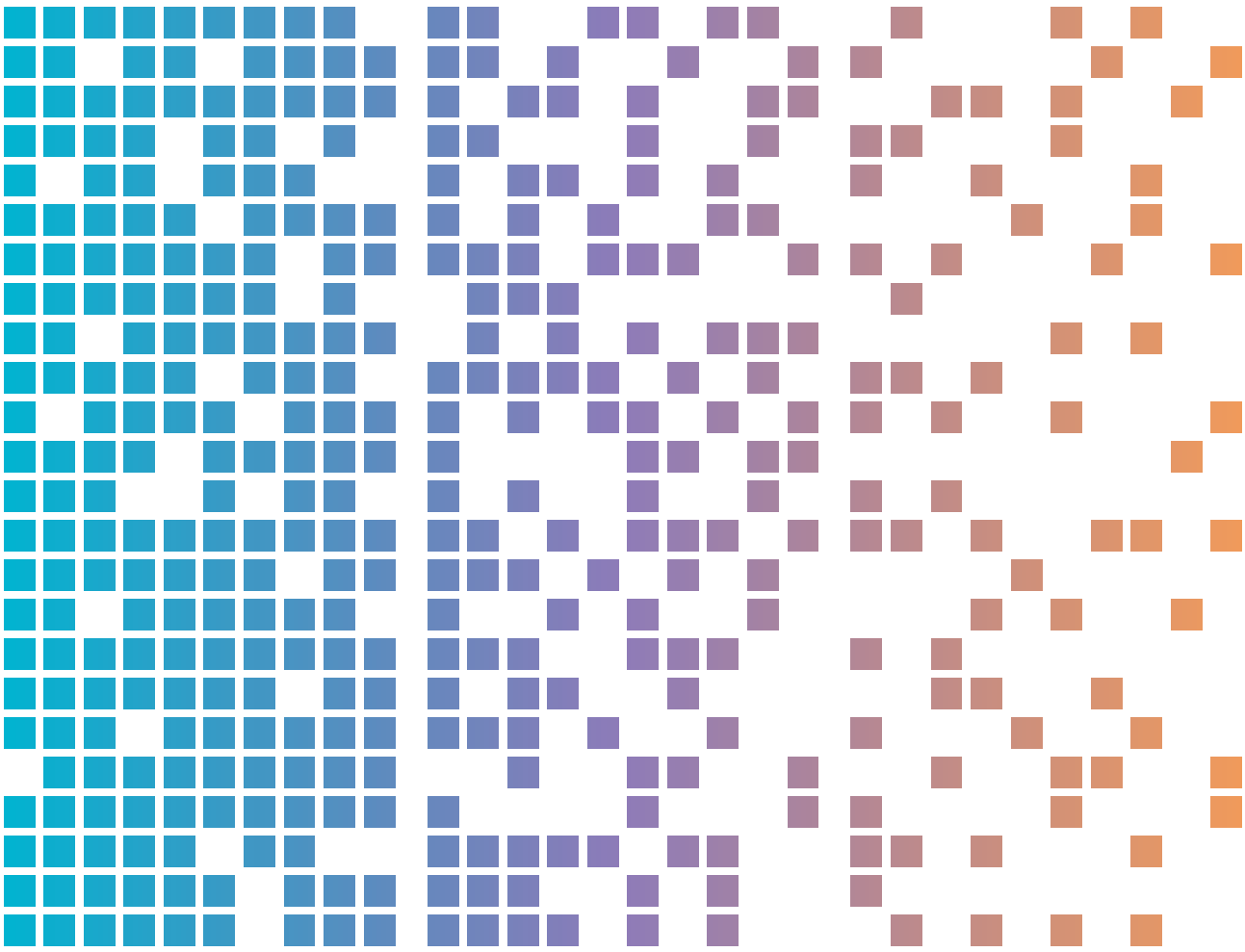
Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Vụ trộm thầm lặng: tội phạm mạng sử dụng phần mềm độc hại đánh cắp dữ liệu để xâm nhập vào hệ thống mạng lưới của các công ty



Mức độ phức tạp của nội dung
VỪA PHẢI ●●○

Mục lục

Tình huống

Phần mềm độc hại đánh cắp các thông tin đăng nhập của người sử dụng và dữ liệu hệ thống và tội phạm mạng sẽ dùng những dữ liệu để khai thác, chủ yếu nhằm mục đích trục lợi tài chính. Các phần mềm độc hại đánh cắp thông tin đã được quan sát thấy trong các cuộc tấn công mạng nhắm vào nhiều tổ chức và các lĩnh vực trên toàn thế giới, bao gồm cả Úc. Tài liệu này cung cấp hướng dẫn an ninh mạng cho người đọc về phần mềm độc hại đánh cắp dữ liệu, bao gồm các hoạt động đe dọa và các biện pháp giảm thiểu rủi ro dành cho tổ chức và nhân viên của họ.

Những điểm chính

- Phần mềm độc hại đánh cắp thông tin, còn được gọi là info stealer, là một loại mã độc được thiết kế để thu thập thông tin từ thiết bị của nạn nhân. Thông tin bị đánh cắp có thể bao gồm tên người sử dụng và mật mã, chi tiết thẻ tín dụng, ví tiền điện tử, tập hồ sơ cục bộ lưu trữ trên thiết bị, cũng như dữ liệu trình duyệt như cookie, tiểu sử truy cập và thông tin điền tự động trong mẫu đơn.
- Tội phạm mạng có thể tìm cách mua và sử dụng các thông tin đăng nhập bị đánh cắp liên quan đến tài khoản doanh nghiệp, để chiếm quyền truy cập ban đầu vào thiết bị của nạn nhân, khách hàng của họ hoặc các hệ thống doanh nghiệp khác. Những hậu quả đối với các tổ chức này có thể bao gồm mã độc tống tiền, tống tiền, tấn công chiếm quyền điều khiển email doanh nghiệp và đánh cắp tài sản trí tuệ.
- Trung tâm An ninh Mạng Úc Trực thuộc Tổng cục Tín hiệu Úc (ASD's ACSC) đã xác định nhiều vụ xâm phạm hệ thống mạng lưới doanh nghiệp bắt nguồn từ việc nhân viên truy cập các nguồn lực làm việc từ thiết bị cá nhân đã bị xâm nhập. Trong nhiều trường hợp, tội phạm mạng đã có được quyền truy cập ban đầu vào mạng doanh nghiệp, bằng cách sử dụng thông tin đăng nhập hợp lệ bị đánh cắp. Các cuộc điều tra của chúng tôi cho thấy những vụ xâm nhập nghiêm trọng thường xảy ra sau khi tội phạm mạng truy cập thành công vào tài khoản người sử dụng có đặc quyền.
- Những tổ chức nào cho phép nhân viên, nhà thầu, nhà cung cấp dịch vụ quản lý hoặc các bên liên quan khác truy cập từ xa vào hệ thống mạng lưới của họ, bao gồm cả việc sử dụng thiết bị cá nhân theo mô hình 'mang thiết bị riêng đến nơi làm việc' (BYOD), cần nhận thức rõ về những rủi ro từ phần mềm độc hại đánh cắp thông tin và cần áp dụng các biện pháp bảo vệ từ những mối đe dọa này. Tội phạm mạng triển khai phần mềm độc hại đánh cắp thông tin (info stealer) lên thiết bị của nạn nhân bằng nhiều kỹ thuật khác nhau, bao gồm: email lừa đảo (phishing), tải phần mềm lậu, kỹ thuật tối ưu hóa công cụ tìm kiếm (SEO), quảng cáo độc hại hoặc các liên kết độc hại được đăng trên nền tảng mạng xã hội. Nhìn chung, các thiết bị được sử dụng cho cả công việc và mục đích cá nhân có nguy cơ bị lây nhiễm cao hơn qua các phương thức này, do hành vi người sử dụng và mức độ kiểm soát bảo mật kém.
- Phần mềm độc hại đánh cắp thông tin là mô hình hấp dẫn để tội phạm mạng kiếm tiền từ hoạt động tấn công mạng, đặc biệt là đối với những kẻ mới vào nghề và có trình độ kỹ thuật hạn chế. Một số tội phạm mạng sẽ quảng cáo sản phẩm phần mềm độc hại đánh cắp thông tin theo mô hình "Phần mềm độc hại dưới dạng dịch vụ" (Malware-as-a-Service – MaaS), thu lệ phí thuê bao hằng tháng cho việc sử dụng.

Bối cảnh

Việc tội phạm mạng sử dụng phần mềm độc hại đánh cắp thông tin là mối đe dọa đối với an ninh và sự ổn định của các tổ chức tại Úc. Các ca 'lây nhiễm' phần mềm độc hại đánh cắp thông tin thường là hoạt động khởi đầu đối với các vấn đề an ninh mạng nghiêm trọng, vì tội phạm mạng sử dụng chúng để thu thập thông tin đăng nhập của người sử dụng. Những thông tin đăng nhập này, đặc biệt là các tài khoản có quyền truy cập vào dịch vụ từ xa có kết nối với Internet, hoặc tài khoản có đặc quyền sẽ bị lợi dụng để khai thác, để tạo điều kiện lấy quyền truy cập ban đầu vào hệ thống và dữ liệu doanh nghiệp.

Ghi chú: Các nhà môi giới quyền truy cập ban đầu (Initial access brokers) đóng một vai trò chuyên biệt trong hệ sinh thái tội phạm mạng, bằng cách mua và xác minh thông tin đăng nhập của người sử dụng bị đánh cắp. Sau đó, họ đấu giá các thông tin đăng nhập với phẩm chất cao này, đặc biệt là thông tin truy cập vào các môi trường doanh nghiệp được các tội phạm mạng săn đón, những kẻ sử dụng các thông tin này để xâm nhập vào hệ thống mạng lưới doanh nghiệp của tổ chức.

Thông tin đăng nhập hợp lệ bị đánh cắp có giá trị rất cao đối với tội phạm mạng, vì chúng giúp đẩy nhanh quá trình truy cập ban đầu vào hệ thống mạng lưới công ty và các hệ thống doanh nghiệp. Khi có được các thông tin đăng nhập hợp lệ, tội phạm mạng có thể vượt qua một số chiến thuật và kỹ thuật thông thường, bao gồm:

- xác nhận và nghiên cứu mục tiêu
- xác định hệ thống mạng lưới của mục tiêu để tìm lỗ hổng bảo mật
- phát triển các phương thức xâm nhập ban đầu, chẳng hạn như:
  - tạo ra nội dung lừa đảo
  - khai thác các lỗ hổng phần mềm
  - nhắm vào các dịch vụ từ xa, bao gồm Giao thức Máy vi tính Từ xa (Remote Desktop Protocol – RDP) hoặc các dịch vụ mạng ảo riêng (Virtual Private Network – VPN)
  - tấn công dò tìm mật mã (brute force) đối với thông tin đăng nhập của người sử dụng.

Những bước này đòi hỏi sự đầu tư về thời gian và trình độ kỹ thuật, đây là rào cản đối với một số tội phạm mạng. Đặc biệt là đối với những tội phạm mạng nào không thể vượt qua được các lớp phòng thủ của hệ thống mạng lưới doanh nghiệp, thì chúng có thể trực tiếp hưởng lợi từ các ca 'lây nhiễm' phần mềm độc hại đánh cắp thông tin, vì các ca 'lây nhiễm' này có thể cung cấp quyền truy cập thông tin đăng nhập của người sử dụng nhanh chóng và dễ dàng vào các hệ thống mạng lưới doanh nghiệp mà chúng hằng mong muốn.

Trong môi trường làm việc từ xa, một số nhân viên sử dụng các thiết bị cá nhân cho cả công việc và việc duyệt mạng cá nhân (internet browsing). Khi làm như vậy, họ có thể chọn lưu trữ thông tin đăng nhập trong bộ lưu trữ mật mã và tiện ích mở rộng của trình duyệt, hoặc sử dụng tính năng tự động điền của trình duyệt mạng. Phần mềm độc hại đánh cắp thông tin nhắm vào các bộ lưu trữ mật mã này, cùng với cookie xác thực và các dữ liệu cá nhân khác bên trong trình duyệt mạng.

Không giống như thiết bị của công ty, thiết bị cá nhân không phải lúc nào cũng được áp dụng các chính sách bảo mật của doanh nghiệp, điều này tạo ra rủi ro cao hơn cho các tổ chức. Ví dụ, nhân viên có thể tham gia vào các hoạt động như tải phần mềm lậu và duyệt mạng với các trang mạng có nguy cơ cao, làm tăng tỷ lệ tiếp xúc với các mối đe dọa mạng và lây nhiễm phần mềm độc hại.

Phần mềm độc hại đánh cắp thông tin, nhà phân phối, các nhà môi giới quyền truy cập ban đầu và đối tác ransomware hiện nay hình thành một phần cốt lõi trong hệ sinh thái tội phạm mạng hoạt động vì lợi nhuận tài chính. Hệ sinh thái này trở nên hiệu quả hơn khi tội phạm mạng chuyên môn hóa và phát triển các năng lực nhắm vào những giai đoạn cụ thể của một cuộc tấn công, sau đó rao bán các năng lực đó như một dịch vụ cho các tổ chức tội phạm khác.

Hoạt động đe dọa

Trung tâm An ninh Mạng Úc Trực thuộc Cục Tín hiệu Úc (ASD's ACSC) đang theo dõi và giám sát sự gia tăng hoạt động của phần mềm độc hại đánh cắp thông tin trên toàn cầu gây ra mối đe dọa ngày càng lớn đối với các hệ thống mạng lưới tại Úc. Phúc trình ngành cho thấy phần mềm độc hại đánh cắp thông tin là biến thể phần mềm độc hại thường gặp nhất trong các hoạt động tội phạm mạng suốt năm 2023. Số lượng dữ liệu bị đánh cắp được rao bán tại các chợ đen trên trang mạng tối (dark web) ngày càng tăng, cùng với sự gia tăng hoạt động của các nhà môi giới quyền truy cập ban đầu tận dụng dữ liệu này, phản ánh xu hướng đang gia tăng này và đã tăng tốc vào năm 2024.

Hệ sinh thái phần mềm độc hại đánh cắp thông tin

Giai đoạn 1: Tìm kiếm phần mềm độc hại

Phần mềm độc hại đánh cắp thông tin thường được rao bán trên các thị trường tội phạm mạng dưới dạng MaaS (phần mềm độc hại dưới dạng dịch vụ) hoặc Stealer-as-a-Service (phần mềm độc hại đánh cắp thông tin dưới dạng dịch vụ), hoặc được bán dưới dạng mã nguồn. MaaS là một mô hình kinh doanh mà nhà phát triển phần mềm độc hại bán gói đăng ký sử dụng phần mềm độc hại của họ cho cá nhân thông qua nền tảng mạng, tương tự như Phần mềm như một Dịch vụ (Software-as-a-Service) hợp pháp. Mô hình MaaS đã hạ thấp rào cản xâm nhập cho tội phạm mạng, vì nó cho phép những người không có kỹ năng kỹ thuật sâu rộng, vẫn có thể phân phối phần mềm độc hại và thu thập thông tin bị đánh cắp để sử dụng trong các cuộc tấn công mạng.

Các phần mềm độc hại đánh cắp thông tin dưới dạng MaaS thường được quảng cáo với mức lệ phí hằng tháng tương đối thấp, và cung cấp cho tội phạm mạng quyền truy cập vào bảng điều khiển (dashboard) của phần mềm độc hại đánh cắp thông tin. Bảng điều khiển tạo điều kiện cho việc tạo ra phần mềm độc hại đánh cắp thông tin, sắp xếp dữ liệu bị đánh cắp và theo dõi số lượng các hệ thống bị xâm phạm. Các nhà điều hành MaaS cung cấp các bản cập nhật tính năng, công cụ và hỗ trợ kỹ thuật để tránh bị phần mềm diệt vi-rút phát hiện và thu hút cũng như để giữ chân người đăng ký. Nhiều phần mềm độc hại đánh cắp thông tin có khả năng tự xóa khỏi thiết bị của nạn nhân sau khi đã thực hiện việc đánh cắp dữ liệu.

Giai đoạn 2: Phân phối

Tội phạm mạng phân phối phần mềm độc hại đánh cắp thông tin và thu thập dữ liệu từ các thiết bị bị xâm nhập được gọi là "Traffers" (nhà phân phối lưu lượng). Traffers dẫn dắt nạn nhân đến các đường dẫn độc hại cho việc phát tán phần mềm độc hại, đánh cắp dữ liệu trong các chiến dịch có quy mô lớn. Phần lớn các chiến dịch này đều không chừa một mục tiêu nào, chỉ nhằm mục đích tìm kiếm cơ hội để lây nhiễm. Tuy nhiên, một số chiến dịch được thiết kế riêng cho các ngành cụ thể và sử dụng kỹ thuật tấn công lừa đảo có mục tiêu (spear-phishing) nhắm vào những nạn nhân cụ thể. Traffers thực hiện các chiến dịch có mục tiêu này theo yêu cầu của khách hàng; ví dụ, khi người mua tìm kiếm quyền truy cập vào các tổ chức hoặc lĩnh vực có giá trị cao.

Traffers sẽ triển khai phần mềm độc hại đánh cắp dữ liệu lên thiết bị của nạn nhân bằng nhiều kỹ thuật khác nhau, bao gồm:

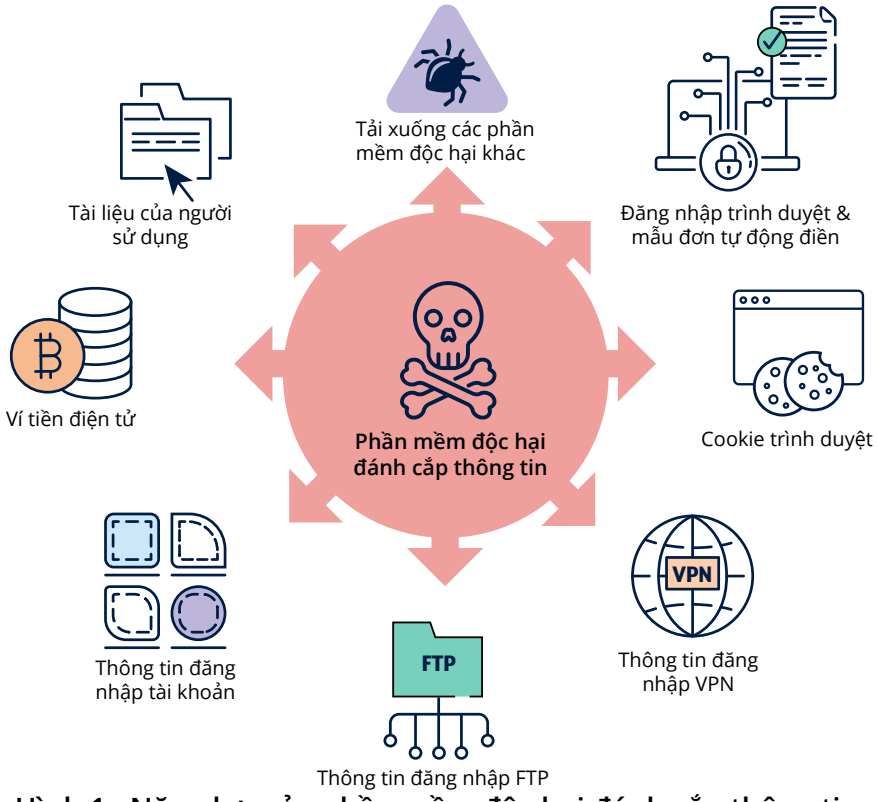
- **botnet**: hệ thống mạng lưới của các hệ thống máy vi tính bị xâm nhập và được tội phạm mạng điều khiển để thực hiện các hành động độc hại, chẳng hạn như phát tán email lừa đảo hoặc phần mềm độc hại

- **phishing**: các nỗ lực lấy thông tin nhạy cảm bằng cách lừa đảo, bao gồm: qua email hoặc tin nhắn trực tiếp trên mạng xã hội, diễn đàn và ứng dụng nhắn tin, đây là các phương thức phân phối thường gặp, giúp hạ thấp rào cản xâm nhập cho tội phạm mạng:
  - Các tin nhắn này thường chứa một đường dẫn độc hại, thay vì đính kèm tập hồ sơ độc hại trực tiếp trong email.
- **kết quả tìm kiếm độc hại**: được phân phối qua các kỹ thuật tối ưu hóa công cụ tìm kiếm (SEO) nhằm dẫn dắt nạn nhân đến các trang mạng chứa phần mềm độc hại giả dạng phần mềm hợp pháp hoặc các nội dung khác
- **quảng cáo độc hại (Malvertising)**: sử dụng mã độc hại được chèn vào các quảng cáo trực tuyến hợp pháp để phát tán phần mềm độc hại
- **phần mềm đã bị bẻ khóa hoặc phần mềm lậu**: các bản tải về, bao gồm cả trò chơi điện tử, được chia sẻ qua YouTube video với đường dẫn độc hại trong phần mô tả hoặc bình luận, hoặc từ các trang mạng để tải xuống không đáng tin cậy
- **quảng cáo và bài đăng trên mạng xã hội**: dẫn dắt nạn nhân đến các tập hồ sơ của phần mềm độc hại được ngụy trang
- **cập nhật phần mềm độc hại**: thường được ngụy trang dưới dạng cập nhật trình duyệt mạng

Giai đoạn 3: Thu thập dữ liệu

Khi phần mềm độc hại đánh cắp thông tin được thực thi trên thiết bị của nạn nhân, nó bắt đầu thu thập dữ liệu nhạy cảm từ máy bị xâm nhập. Ngoài việc đánh cắp thông tin đăng nhập, trong trường hợp phần mềm độc hại đánh cắp thông tin là một phần của mạng botnet, tội phạm mạng có thể điều khiển thiết bị bị xâm nhập từ xa, bằng cách gởi lệnh cấu hình để khởi động các chức năng bổ sung hoặc phát tán phần mềm độc hại khác. Thông thường, phần mềm độc hại đánh cắp thông tin có khả năng lấy cắp các loại dữ liệu sau:

- tên người sử dụng và mật mã, đặc biệt là những thông tin được lưu trong các phiên/ mã thông báo xác thực đa yếu tố (MFA) của trình duyệt mạng
- cookie xác thực
- thông tin của mẫu đơn tự động điền trên trình duyệt mạng
- thông tin đăng nhập email, nội dung email và danh bạ
- tiểu sử duyệt mạng
- tài liệu người sử dụng• thông tin về thẻ tín dụng
- nhật ký ghi chép trò chuyện từ các ứng dụng nhắn tin trên máy vi tính để bàn
- thông tin hệ thống•ví tiền điện tử
- Thông tin đăng nhập VPN hoặc Giao thức Truyền tải Tập Hồ sơ (FTP).



Hình 1. Năng lực của phần mềm độc hại đánh cắp thông tin

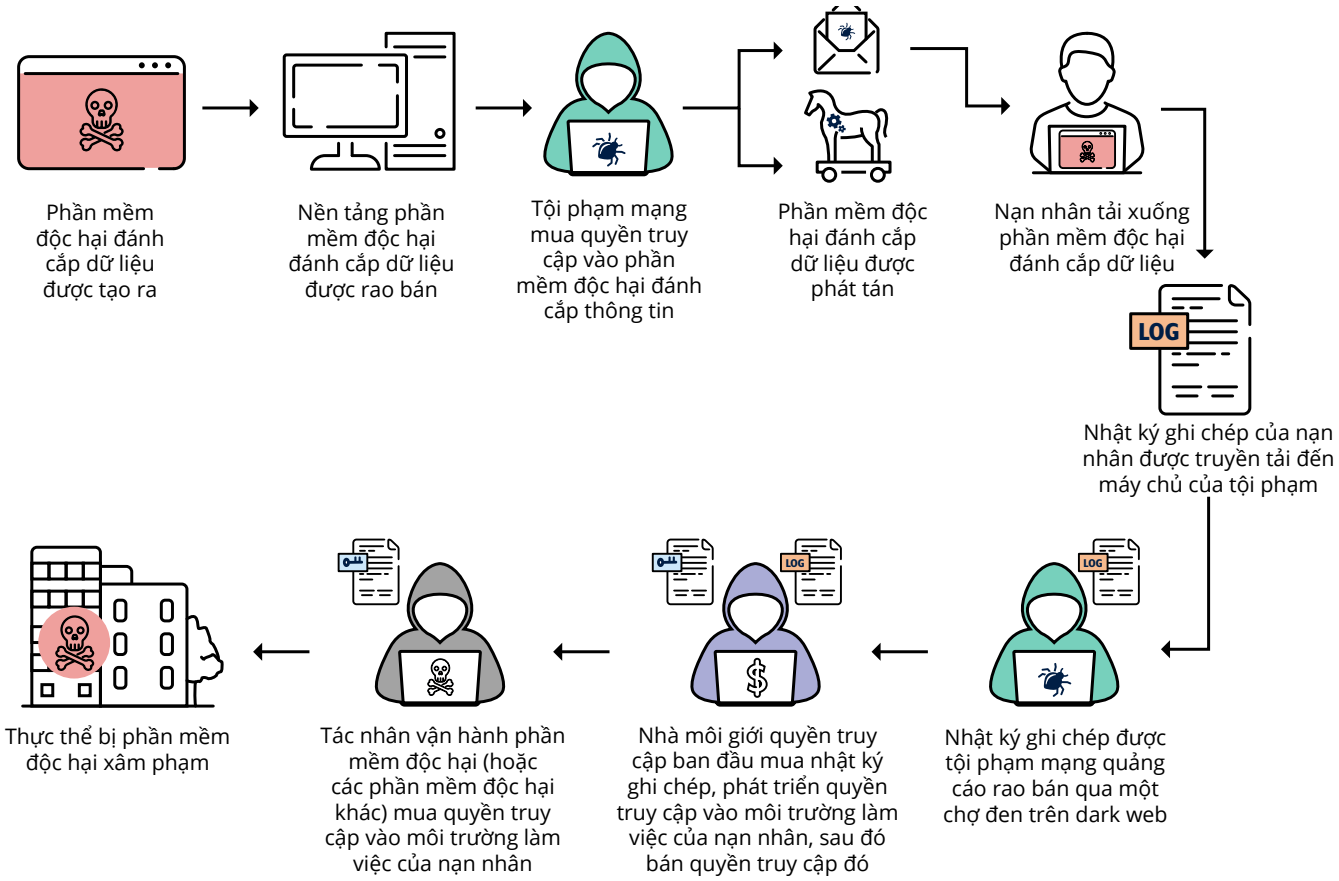
Một số cookie xác thực trên trình duyệt mạng giúp người sử dụng duy trì trạng thái đăng nhập vào tài khoản hoặc dịch vụ trong nhiều ngày liên tục, do đó người dùng không cần phải xác thực lại nhiều lần. Nếu bị đánh cắp, các cookie xác thực này có thể giúp tội phạm mạng vượt qua yêu cầu xác thực đa yếu tố (MFA) một cách hiệu quả và truy cập vào tài khoản của nạn nhân, hệ thống mạng lưới của công ty cũng như hệ thống của doanh nghiệp.

Giai đoạn 4: Tích lũy dữ liệu và kiếm tiền từ dữ liệu

Phần mềm độc hại đánh cắp thông tin được cấu hình để trích đánh cắp dữ liệu của nạn nhân được mang tên là “nhật ký ghi chép" ('logs'), gởi về các máy chủ điều khiển và chỉ huy độc hại. Thông thường, các phần mềm độc hại đánh cắp thông tin sử dụng các ứng dụng nhắn tin phổ biến như Telegram và Discord, để chia sẻ luồng nhật ký ghi chép với tội phạm mạng.

Trên Telegram và khắp dark web tồn tại các thị trường chuyên biệt để mua bán và trao đổi luồng nhật ký ghi chép. Tội phạm mạng kiếm tiền từ các nhật ký ghi chép theo nhiều cách khác nhau, bao gồm:

- bán nhật ký ghi chép trên các thị trường tội phạm, trong đó có cả các nhà môi giới quyền truy cập ban đầu
- khai thác trực tiếp nạn nhân thông qua việc đánh cắp danh tính và tống tiền
- sử dụng thông tin để truy cập ban đầu vào hệ thống mạng lưới doanh nghiệp nhằm thực hiện các hoạt động của phần mềm độc hại.



Hình 2. Hệ sinh thái phần mềm độc hại đánh cắp thông tin và tác động có thể xảy ra đối với một tổ chức

Hệ quả

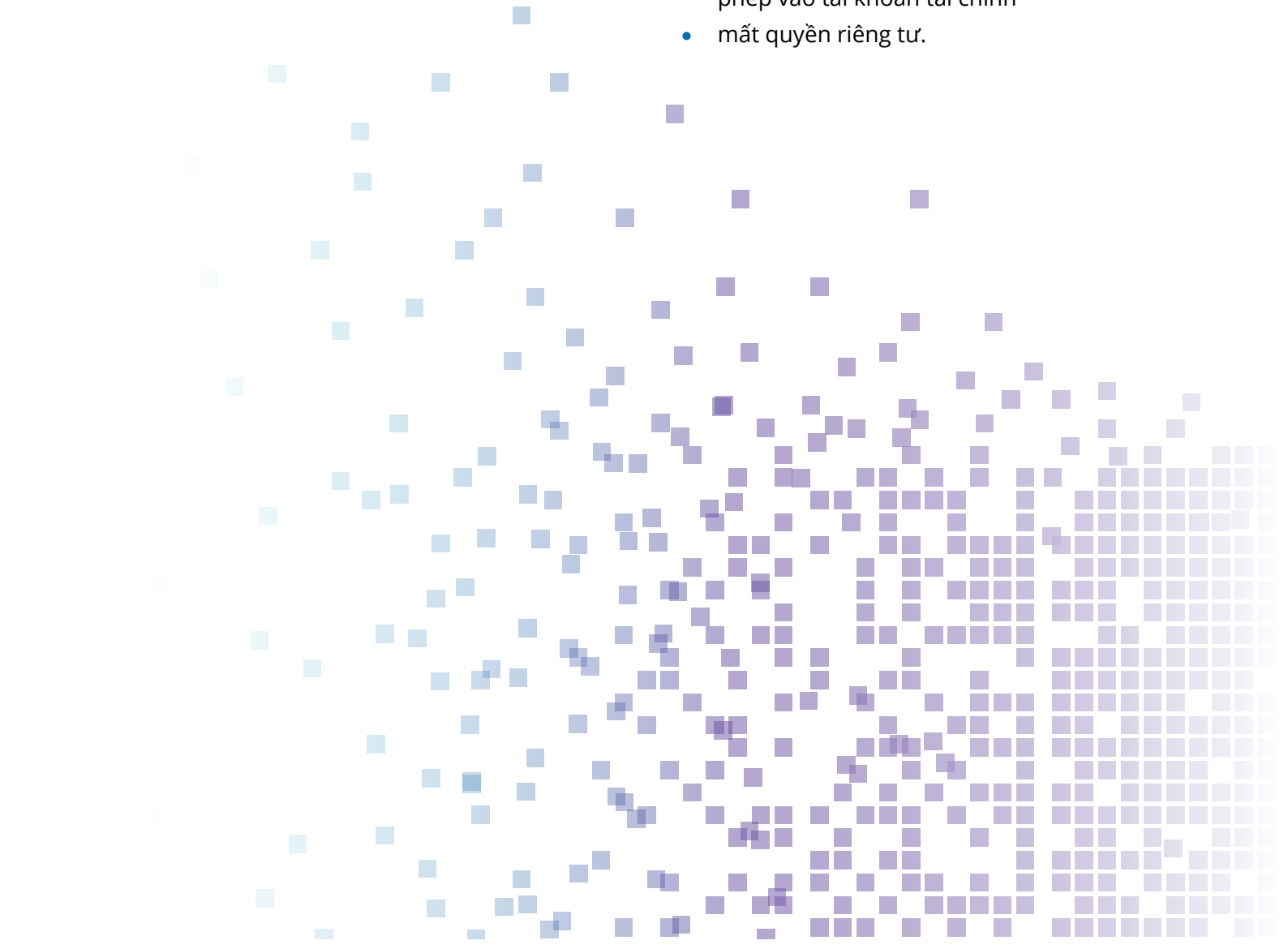
Phần mềm độc hại đánh cắp thông tin có thể gây ra những hậu quả nghiêm trọng đối với cả cá nhân và tổ chức. Khi phần mềm độc hại đánh cắp thông tin thu thập thông tin đăng nhập của người sử dụng. Tội phạm mạng có thể sử dụng các thông tin này để truy cập hệ thống mạng lưới công ty hoặc hệ thống doanh nghiệp với các tài khoản hợp lệ, thường làm chậm việc phát hiện của chủ sở hữu hệ thống.

Đối với **các tổ chức** bị ảnh hưởng bởi phần mềm độc hại đánh cắp thông tin, các hậu quả có thể bao gồm:

- phần mềm tống tiền
- xâm phạm dữ liệu
- xâm phạm email doanh nghiệp
- trộm cắp tài sản trí tuệ
- trộm cắp thông tin nhạy cảm.

Đối với **cá nhân** bị ảnh hưởng bởi phần mềm độc hại đánh cắp dữ liệu, hậu quả có thể bao gồm:

- truy cập trái phép vào email cá nhân hoặc tài khoản mạng xã hội
- gia tăng nguy cơ bị đánh cắp danh tính
- gia tăng nguy cơ bị tấn công lừa đảo
- tổn thất tài chính hoặc truy cập trái phép vào tài khoản tài chính
- mất quyền riêng tư.



Nghiên cứu trường hợp điển hình

Nghiên cứu điển hình này đã được ẩn danh nhằm cho phép công khai. Nội dung dựa trên nhiều vấn đề an ninh mạng đã ảnh hưởng đến các thực thể tại Úc và được trình báo cho Trung tâm An ninh Mạng Úc Trực thuộc Cục Tín hiệu Úc (ASD's ACSC). Thực thể bị ảnh hưởng kể từ đây sẽ được gọi là "tổ chức". Tên của các cá nhân trong nghiên cứu điển hình này là giả định và các chi tiết đã được loại bỏ nhằm bảo vệ danh tính của các nạn nhân.

Tổ chức này là một doanh nghiệp tại Úc cho phép nhân viên truy cập hệ thống doanh nghiệp từ thiết bị cá nhân. Alice là một nhân viên của tổ chức và làm việc từ xa.

Khi làm việc tại nhà, Alice truy cập hệ thống mạng lưới doanh nghiệp của tổ chức mình từ xa bằng chiếc máy vi tính xách tay cá nhân của cô. Alice **đã tải xuống**, vào trong **máy vi tính xách tay cá nhân** của cô ấy, một phiên bản Notepad++ (một loại phần mềm ghi chú) từ một trang mạng mà cô ấy tin là hợp pháp. Một **phần mềm độc hại đánh cắp thông tin** đã được ngụy trang thành dưới dạng bộ cài đặt phần mềm Notepad++.

Khi Alice cố gắng cài đặt phần mềm này, thì phần mềm độc hại đánh cắp thông tin đã khởi động và bắt đầu **thu thập thông tin đăng nhập của người sử dụng** từ chiếc máy vi tính xách tay cá nhân của cô. Những dữ liệu này bao gồm, tên đăng nhập và mật mã công việc của cô, được cô lưu trữ trong tính năng đăng nhập đã lưu trữ của trình duyệt mạng. Phần mềm độc hại đánh cắp dữ liệu sau đó gởi các thông tin đăng nhập này đến một máy chủ điều khiển và chỉ huy từ xa, do một nhóm tội phạm mạng kiểm soát.

Các nhật ký ghi chép bị đánh cắp được đóng gói cùng với các nhật ký ghi chép khác rồi **bán cho tội phạm mạng** qua một chợ đen trên dark web.

Một tội phạm mạng tên là Bob đã mua các thông tin đăng nhập của Alice, xác định các thông tin đăng nhập cho các dịch vụ trong hệ thống mạng lưới của tổ chức cô. Tổ chức của Alice đã **không cấu hình xác thực đa yếu tố (MFA)** cho những dịch vụ này, điều đó có nghĩa là Bob có thể sử dụng riêng thông tin đăng nhập hợp lệ bị đánh cắp để **xác thực và truy cập thành công** vào hệ thống mạng lưới doanh nghiệp.

Bob đã truy cập hệ thống mạng lưới doanh nghiệp của tổ chức Alice mà không bị phát hiện, sử dụng các **thông tin đăng nhập hợp lệ** bị đánh cắp. Bob có thể di chuyển hàng ngang trong hệ thống mạng lưới doanh nghiệp, xác định dữ liệu nhạy cảm thuộc về tổ chức và đánh cắp để tống tiền công ty.

Sau khi đánh cắp thông tin nhạy cảm, Bob đã **mã hóa** các **cơ sở dữ liệu và hệ thống tập hồ sơ tin** của tổ chức để làm cho chúng không thể được truy cập.

Biện pháp giảm thiểu rủi ro

Các tổ chức có thể không kiểm soát được các thiết bị kết nối vào hệ thống mạng lưới doanh nghiệp của mình, đặc biệt là các thiết bị cá nhân được nhân viên làm việc từ xa sử dụng. Trung tâm An ninh Mạng Úc Trực thuộc Cục Tín hiệu Úc (ASD's ACSC) khuyến cáo các tổ chức tập nên trung triển khai các biện pháp kiểm soát, nhằm bảo vệ mình từ nguy cơ phần mềm độc hại đánh cắp thông tin nhắm vào thông tin đăng nhập người sử dụng. Biện pháp giảm thiểu rủi ro này bao gồm:

Đào tạo nhận thức về an ninh mạng cho nhân viên

- Ngăn chặn các hoạt động tấn công xã hội có chủ đích và việc tải xuống các tập hồ sơ độc hại bằng cách đào tạo hiệu quả cho nhân viên.
- Nâng cao nhận thức về phần mềm độc hại đánh cắp thông tin, các phương thức phát tán của chúng và các mối đe dọa lừa đảo đối với tổ chức của quý vị.

Bảo mật tài khoản doanh nghiệp

- Triển khai xác thực đa yếu tố (MFA):
- Triển khai MFA cho tất cả các dịch vụ, hệ thống bên ngoài và nội bộ cũng như các kho lưu trữ dữ liệu nhạy cảm, đặc biệt là đối với thư mạng, VPN, và các tài khoản người dùng có đặc quyền truy cập hệ thống quan trọng. Thực hành tốt nhất là áp dụng MFA chống lừa đảo cho tất cả các tài khoản.
- Vô hiệu hóa tài khoản người sử dụng khi không còn cần thiết nữa.
- Hạn chế đặc quyền quản trị viên:
- Chỉ thực hiện quản trị hệ thống mạng lưới và các nhiệm vụ có đặc quyền trên một máy trạm chuyên dụng và được khóa chặt (tức là máy trạm quản trị an toàn).
- Thực hiện nguyên tắc đặc quyền tối thiểu bằng cách yêu cầu quản trị viên sử dụng tài khoản người sử dụng có đặc quyền để quản lý hệ thống và sử dụng tài khoản người sử dụng thông thường cho các nhiệm vụ không mang tính quản trị.
- Ngăn chặn các tài khoản có đặc quyền (ngoại trừ những tài khoản được cấp quyền truy cập rõ ràng vào dịch vụ trực tuyến) truy cập vào internet, email và các dịch vụ mạng.
- Xem xét việc triển khai mô hình quản trị đúng thời điểm (just-in-time administration) cho hệ thống và ứng dụng.
- Thực hành việc quản lý và giám sát các tài khoản người sử dụng có đặc quyền.
- Thường xuyên cập nhật mật mã, đặc biệt là đối với các tài khoản truy cập từ xa có khả năng kết nối với bên ngoài.
- Áp dụng giới hạn thời gian sử dụng và chính sách hết hạn đối với các mã phiên (session tokens) và cookie.

Tăng cường bảo mật tính di động của doanh nghiệp

- Thực hiện đánh giá rủi ro về thiết bị di động trong doanh nghiệp và triển khai hướng dẫn tăng cường bảo mật tính di động của doanh nghiệp.
- Triển khai chính sách mang thiết bị riêng đến nơi làm việc (BYOD) nếu tổ chức cho phép nhân viên sử dụng thiết bị cá nhân cho công việc, vì thiết bị được quản lý bởi doanh nghiệp thường an toàn hơn so với thiết bị cá nhân không được kiểm soát.

Xem xét và đánh giá rủi ro chuỗi cung ứng từ các nhà cung cấp có quyền truy cập vào hệ thống mạng lưới của quý vị, bao gồm cả nhà cung cấp dịch vụ phần mềm dưới dạng dịch vụ (SaaS) và nhà cung cấp dịch vụ được quản lý (Managed Service Providers). Cách Quản lý Bảo mật Khi Hợp tác với Nhà Cung cấp Dịch vụ được Quản lý.

Bảo vệ hệ thống mạng lưới nội bộ doanh nghiệp

- Luôn cập nhật ứng dụng và hệ điều hành.
- Áp dụng chính sách bảo mật cục bộ để thực hiện kiểm soát ứng dụng thông qua danh sách cho phép nghiêm ngặt (strict allow list).
- Triển khai phân đoạn hệ thống mạng lưới để tách biệt các phân đoạn mạng dựa trên vai trò và chức năng.
- Kiểm tra và giám sát hoạt động của người sử dụng, đặc biệt là đối với nhân viên làm việc từ xa.
- Giám sát các tài khoản có đặc quyền có thể giúp phát hiện truy cập trái phép vào dữ liệu nhạy cảm hoặc các hoạt động truyền tải dữ liệu bất thường, chẳng hạn như tải lên một lượng lớn dữ liệu tới mạng bên ngoài.
- Triển khai các chính sách và công cụ ngăn chặn rò rỉ dữ liệu để ngăn chặn các hành vi truyền tải dữ liệu trái phép.

Trở thành Đối tác của Hệ thống Mạng lưới An ninh mạng của Tổng cục Tín hiệu Úc (ASD) và dịch vụ Chia sẻ Tình báo Mối Đe dọa Mạng (CTIS)

- CTIS là một nền tảng chia sẻ hai chiều, cho phép các đối tác chính phủ và doanh nghiệp nhận và chia sẻ thông tin về hoạt động mạng độc hại.
- Trung tâm An ninh Mạng Úc Trực thuộc Tổng cục Tín hiệu Úc (ASD's ACSC) đang theo dõi hoạt động của phần mềm độc hại đánh cắp thông tin và chia sẻ chi tiết về các hạ tầng cơ sở điều khiển và chỉ huy đang hoạt động thông qua nền tảng CTIS.
- Đăng ký trở thành đối tác để bảo vệ tổ chức và dữ liệu khách hàng của quý vị khỏi các mối đe dọa từ tội phạm mạng.

Chuẩn bị cho sự xâm nhập

- Phát triển kế hoạch đối phó với các vấn đề an ninh mạng để sử dụng trong trường hợp bị phần mềm độc hại đánh cắp dữ liệu xâm nhập. Hãy bảo đảm rằng nhân viên biết phải làm gì và liên lạc với ai nếu họ nghi mình đã tải xuống một tập hồ sơ đáng nghi ngờ.

Triển khai Tám Chiến lược Giảm thiểu Thiết yếu của Trung tâm An ninh Mạng Úc Trực thuộc Tổng cục Tín hiệu Úc (ASD's ACSC)

- Ngoài các biện pháp giảm thiểu rủi ro đã nêu ở trên, Trung tâm An ninh Mạng Úc Trực thuộc Tổng cục Tín hiệu Úc (ASD's ACSC) khuyến cáo mạnh mẽ việc triển khai đầy đủ bộ Tám Chiến lược Giảm thiểu Thiết yếu của họ.

Lời khuyên dành cho nhân viên khi làm việc từ xa

- Bảo vệ thông tin trên thiết bị cá nhân của quý vị
  - Thực hiện 'vệ sinh mạng' (cyber hygiene) tốt, và không nhấp vào các đường dẫn hoặc cửa sổ bật lên đáng nghi ngờ, hoặc tải xuống tập hồ sơ hoặc phần mềm từ các nguồn chưa được xác định hoặc không đáng tin cậy.
  - Sử dụng mật mã khác nhau cho các tài khoản công việc và cá nhân. Bật xác thực đa yếu tố (MFA) cho các tài khoản cá nhân bất cứ khi nào có thể.
  - Không lưu trữ thông tin đăng nhập công việc của quý vị vào trình quản lý mật mã cá nhân, trừ khi được công ty cho phép một cách rõ ràng. Điều này bao gồm cả trình quản lý mật mã của trình duyệt mạng của quý vị. **Nếu không chắc chắn, hãy yêu cầu công ty cung cấp một trình quản lý mật mã được doanh nghiệp hỗ trợ.**
  - Không đăng nhập vào tài khoản công việc từ các máy vi tính sử dụng chung hoặc nơi làm việc công cộng.
  - Hãy lưu ý đến những gì đang được lưu trữ trong tính năng tự động điền của trình duyệt mạng của quý vị. Phần mềm độc hại đánh cắp thông tin nhắm vào thông tin mà trình duyệt lưu trữ để tự động điền vào mẫu đơn. Khi điền mẫu đơn mạng, hãy xem xét việc tự tay điền các thông tin nhạy cảm, chẳng hạn như số thẻ tín dụng, thay vì lưu chúng vào tính năng tự động điền của trình duyệt.
  - Đăng xuất khỏi tất cả các dịch vụ trực tuyến và xóa cookie trình duyệt sau khi kết thúc phiên duyệt mạng để giảm lượng thông tin có thể bị phần mềm độc hại đánh cắp thông tin khai thác.
  - Hãy bảo đảm phần mềm chống vi-rút tích hợp sẵn của hệ điều hành của quý vị đã được bật lên. Nếu quý vị sử dụng phần mềm chống vi-rút của bên thứ ba, hãy bảo đảm rằng phần mềm đó luôn được cập nhật và đến từ nhà cung cấp uy tín.

Giúp đỡ

Các tổ chức tại Úc bị ảnh hưởng hoặc cần giúp đỡ về vấn đề bị phần mềm độc hại đánh cắp thông tin xâm nhập, có thể liên lạc với Trung tâm An ninh Mạng Úc Trực thuộc Tổng cục Tín hiệu Úc (ASD's ACSC) qua số **1300 CYBER1 (1300 292 371)** hoặc gởi phúc trình tại cyber.gov.au/report.

Trung tâm An ninh Mạng Úc Trực thuộc Tổng cục Tín hiệu Úc (ASD's ACSC) khuyến khích các tổ chức trình báo các hoạt động mạng đáng nghi ngờ và các dấu hiệu bị xâm nhập liên quan đến phần mềm độc hại đánh cắp thông tin, ngay cả khi vấn đề được cho là đã được giải quyết. Thông tin quý vị cung cấp giúp chúng tôi hiểu rõ hơn về các chiến thuật, kỹ thuật và phương sách của các tác nhân đe dọa mạng, từ đó giúp đỡ cảnh báo các tổ chức khác tại Úc đang bị nhắm mục tiêu theo cách tương tự.

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 được 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 trông cậy vào thông tin có trong hướng dẫn này.

Muốn biết thêm thông tin, hoặc muốn trình báo vấn đề an ninh mạng, 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