

|  |
| --- |
| ATT&CK Project |
| Discovery Whitepaper  *v1.0 - 02/04/2021* |
| Phòng mã độc và khai thác lỗi  Công ty An ninh mạng Viettel  Authored by: HuyHv9 |



ATT&CK Project

Discovery Whitepaper

# Tổng quan

Attacker sử dụng kĩ thuật này để tìm hiểu về môi trường máy nạn nhân.

Discovery bao gồm những kĩ thuật một attacker có thể sử dụng để thu thập thông tin về hệ thống và mạng nội bộ. Những kĩ thuật này giúp attacker theo dõi môi trường và tự mình điều hướng trước khi quyết định cách hành động. Chúng cũng cho phép attacker khám phá những gì có thể điều khiển và những gì xung quang điểm vào (entry point) để khám phá lợi ích nó có thể đem lại cho đối tượng hiện tại. Các công cụ hệ thống được sử dụng để thu thập thông tin đối tượng.

# Mô tả kỹ thuật chi tiết

## [T1087] Account Discovery

* 1. Local Account:
* Attacker cố gắng để liệt kê local system account. Các thông tin này có thể giúp attacker xác định những tài khoản nào đang tồn tại trên hệ thống để điều hướng tấn công.
* Cách thức triển khai:
  + Cmd:

net user

net localgroup

* + PowerShell:

Get-LocalGroup

Get-LocalUser

* 1. Domain Account:
* Attacker cố gắng để liệt kê domain system account. Các thông tin này có thể giúp attacker xác định những tài khoản domain nào đang tồn tại trên hệ thống để điều hướng tấn công.
* Cách thức triển khai:
  + Cmd:

net user /domain

net group /domain

* + Powershell:

Get-ADUser

Get-ADDomain

* 1. Email Account:
* Attacker cố gắng liệt kê các tài khoảng và địa chỉ email. Attacker cố gắng dump danh sách địa chỉ Exchange như danh sách địa chỉ cục bộ (GALs).
* Cách thức triển khai:
  + Powershell:

Get-GlobalAddressList

1. [T1010] Application Window Discovery

* Attacker cố gắng có được danh sách của các cửa sổ ứng dụng đang chạy. Cửa sổ đang được liệt kê có thể mang thông tin về cách hệ thống được sử dụng hoặc gửi nội dung cho thông tin được thu thập bởi keylogger.
* Cách thức triển khai:
  + Powershell:

Get-Process | Where-Object {$\_.MainWindowTitle -ne ""} | Select-Object MainWindowTitle

1. [T1217] Browser Bookmark Discovery

* Attacker liệt kê các dấu trang trong trình duyệt để biết nhiều hơn về máy chủ bị tấn công. Dấu trang trình duyệt có thể tiếp cận thông tin cá nhân của người sử dụng cũng như những tài nguyên mạng nội bộ như server, công cụ,...
* Dấu trang trình duyệt cũng có thể làm nổi bật các mục tiêu bổ sung sau khi attacker có quyền truy cập vào thông tin đăng nhập hợp lệ, đặc biệt là Thông tin đăng nhập trong Tệp được liên kết với thông tin đăng nhập được trình duyệt lưu trong bộ nhớ cache.
* Cách thức triển khai:
  + Powershell:

Get-Content "C:\Users\\*\AppData\Local\Google\Chrome\User Data\Default\Bookmarks"

1. [T1482] Domain Trust Discovery

* Attacker cố gắng thu thập thông tin trên những mối quan hệ tin cậy miền có thể sử dụng để xác định cơ hội di chuyển trong môi trường nhiều miền của Windows.
* Cách thức triển khai:
  + Powershell:

Get-ADTrust

1. [T1083] File and Directory Discovery

* Attacker cố gắng liệt kê các têp và thư mục hoặc có thể tìm kiếm trong những địa điểm cụ thể của một máy chủ lưu trữ hoặc mạng chia sẻ để tìm thông tin nhất định trong hệ thống tệp. Attacker có thể sử dụng thông tin từ File and Directory Discovery để định hình các hành vi tiếp theo.
* Cách thức triển khai:
  + Powershell or Cmd:

Dir

1. [T1135] Network Share Discovery

* Attacker có thể tìm kiếm thư mục và ổ đĩa được chia sẻ trên hệ thống từ xa như là một phương tiện xác định nguồn thông tin để thu thập làm tiền than cho việc thu thập và để xác định hệ thống tiền năng quan tâm đến Lateral Movement.
* Cách thức triển khai:
  + Cmd:

net view \remotesystem

net share

1. [T1201] Password Policy Discovery

* Attacker cố gắng truy cập thông tin chi tiết về chính sách password được sử dụng bên trong mạng doanh nghiệp. Dựa trên chính sách này để tấn công bruteforce hiệu quả hoặc thiết lâp danh sách password thông dụng.
* Cách thức triển khai:
  + Cmd:

net accounts (/domain)

* + Powershell:

Get-ADDefaultDomainPasswordPolicy

1. [T1120] Peripheral Device Discovery

* Attacker cố gắng thu thập thông tin về các thiết bị ngoại vi đính kèm và các thành phần được kết nối với hệ thống máy tính. Các thiết bị ngoại vi có thể bao gồm các tài nguyên phụ trợ hỗ trợ nhiều chức năng khác nhau như bàn phím, máy in, máy ảnh, đầu đọc thẻ thông minh hoặc bộ nhớ di động. Thông tin có thể được sử dụng để nâng cao nhận thức của họ về hệ thống và môi trường mạng hoặc có thể được sử dụng cho các hành động tiếp theo.
* Cách thức triển khai:
  + Powershell:

Get-PnpDevice

1. [T1069] Permission Groups Discovery

* Attacker có thể cố gắng tìm cài đặt nhóm và quyền. Thông tin này có thể giúp Attacker xác định tài khoản và nhóm người dùng nào có sẵn, tư cách thành viên của người dùng trong các nhóm cụ thể và người dùng và nhóm nào có quyền cao hơn.
* Cách thức triển khai:
  + Powershell:

Get-ADGroup

Get-LocalGroup

1. [T1057] Process Discovery

* Attacker cố gắng lấy thông tin về các process đang chạy trên hệ thống. Thông tin lấy đc có thể sử dụng để attacker hiểu hơn về các phần mềm và ứng dụng thông thường đang chạy trên hệ thống bên trong mạng. Attacker sử dụng các thông tin từ Process Discovery trong quá trình khám phá tự động để định hình các hành vi tiếp theo.
* Cách thức triển khai:
  + Powershell:

Get-Process

1. [T1012] Query Registry

* Attacker cố gắng tương tác với Windows Registry để thu thập thông tin về hệ thống, cấu hình và những phần mềm đã cài đặt.
* Cách thức triển khai:
  + Powershell:

Get-ItemProperty <key>

* + Cmd:

Reg query <key>

1. [T1082] System Information Discovery

* Attacker cố gắng để lấy thông tin chi tiết về hệ điều hành và phần cứng. Attacker sử dụng các thông tin từ System Information Discovery trong quá trình khám phá tự động để định hình các hành vi tiếp theo.
* Cách thức triển khai:
  + Powershell:

Get-ComputerInfo

* + Cmd:

systeminfo

1. [T1016] System Network Configuration Discovery

* Attacker có thể tìm kiếm chi tiết về cấu hình mạng và cài đặt của hệ thống mà chúng truy cập hoặc thông qua việc khám phá thông tin của các hệ thống từ xa. Một số tiện ích quản trị hệ điều hành có thể được sử dụng để thu thập thông tin này.
* Attacker sử dụng các thông tin từ System Network Configuration Discovery trong quá trình khám phá tự động để định hình các hành vi tiếp theo.
* Cách thức triển khai:
  + Powershell and Cmd:

Ipconfig | ipconfig /all

1. [T1049] System Network Connections Discovery

* Attacker có thể cố gắng lấy danh sách các kết nối mạng đến hoặc từ hệ thống bị xâm nhập mà chúng hiện đang truy cập hoặc từ các hệ thống từ xa bằng cách truy vấn thông tin qua mạng. Attacker có quyền truy cập vào hệ thống là một phần của môi trường dựa trên đám mây có thể vạch ra các Virtual Private Cloud hoặc Virtual Networks để xác định hệ thống và dịch vụ nào được kết nối. Các hành động được thực hiện có thể là các loại kỹ thuật khám phá giống nhau tùy thuộc vào hệ điều hành, nhưng thông tin kết quả có thể bao gồm các chi tiết về môi trường Cloud được nối mạng có liên quan đến mục tiêu của Attacker.
* Cách thức triển khai:
  + Powershell and Cmd:

Net session | net use

1. [T1033] System Owner/User Discovery

* Attacker có thể cố gắng xác định người dùng chính, người dùng hiện đang đăng nhập, nhóm người dùng thường sử dụng hệ thống hoặc liệu người dùng có đang tích cực sử dụng hệ thống hay không. Attacker có thể sử dụng thông tin từ System Owner/User Discovery người dùng trong quá trình khám phá tự động để định hình các hành vi tiếp theo, bao gồm việc liệu attacker có lây nhiễm hoàn toàn mục tiêu hay không và / hoặc thực hiện các hành động cụ thể.
* Cách thức triển khai:
  + Powershell and Cmd:

whoami

1. [T1007] System Service Discovery

* Attacker cố gắng lấy thông tin về các services đã đăng kí. Từ các thông tin lấy đc này, Attacker sẽ quyết định hành động tiếp theo.
* Cách thức triển khai:
  + Powershell:

Get-Service

* + Cmd:

Sc query | net start

1. [T1124] System Time Discovery

* Attacker có thể lấy thông tin về thời gian hệ thống hoặc time zone trên một hệ thống từ xa hoặc local. Thông tin này có ích cho thực thi các kĩ thuật khác, ví dụ như Scheduled Task/Job.
* Cách thức triển khai:
  + Powershell:

Get-Date

Get-TimeZone

# Cách thức phòng chống

<Defend>

# Cách thức phát hiện

<Detect >