BÁO CÁO ĐIỀU TRA VÀ PHÂN TÍCH SỰ CỐ MÃ ĐỘC RAT-20260122T041817Z-3-001

I. THÔNG TIN MÔI TRƯỜNG

1. Đối tượng bị ảnh hưởng

- **Hostname:** DESKTOP-KF7SGRB
- **IP Address:** 192.168.56.129
- **Hệ điều hành:** Windows 10 (Architecture: x64)
- **Vai trò:** Máy trạm của người dùng

2. Công cụ giám sát & Thu thập

- **Hệ thống SIEM:** Wazuh Security Platform.
- **Module sử dụng:** File Integrity Monitoring (FIM) và EventLog.
- **Wazuh Server:** wazuh-server.

II. PHÂN TÍCH MỐI ĐE DỌA

Trước khi đi sâu vào phân tích hành vi trên máy, chúng ta sẽ thực hiện tra cứu mẫu mã độc dựa trên mã băm (Hash) thu thập được.

- **Sample Hash SHA-256:** 6da3064773edf094f014b7aa13f2e3f74634f62552a91f88bf306f962bbf0563
- **Nguồn tham chiếu:** VirusTotal Analysis

Kết quả nghiên cứu cộng đồng:

Dựa trên cơ sở dữ liệu mối đe dọa toàn cầu, mẫu mã độc này được xác định là công cụ **"Defender Control" (dControl.exe)** hoặc một biến thể của nó.

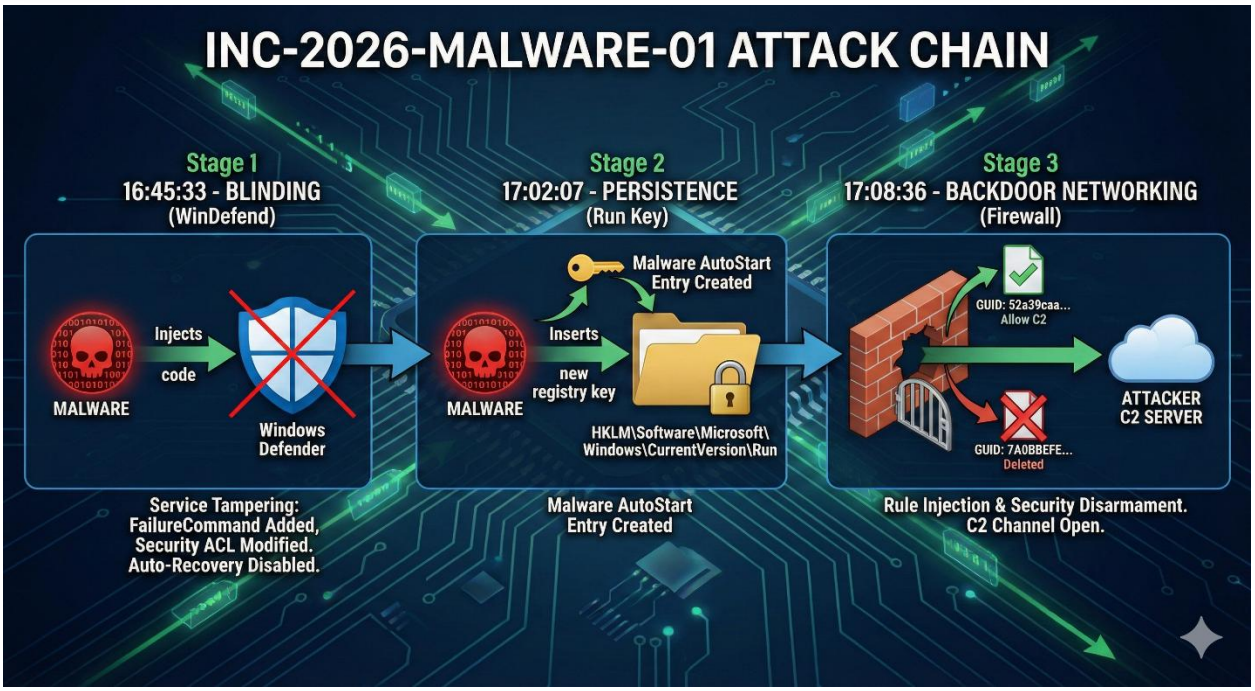
1. **Phân loại: HackTool / PUA (Potentially Unwanted Application)**. Mặc dù đôi khi được dùng bởi quản trị viên, nhưng trong ngữ cảnh này, nó đóng vai trò là vũ khí **Defense Evasion (Lẩn tránh phòng thủ)**.
2. **Hành vi đặc trưng:**

- Cộng đồng bảo mật ghi nhận công cụ này chuyên nhắm vào việc vô hiệu hóa vĩnh viễn **Windows Defender** thông qua Registry và Group Policy.
- Nó thường được các nhóm tấn công (Threat Actors) sử dụng ở **Giai đoạn đầu (Initial Phase)** của chuỗi tấn công để "dọn đường" cho các mã độc nguy hiểm hơn (RAT, Ransomware) xâm nhập mà không bị phát hiện.

III. DÒNG THỜI GIAN TẤN CÔNG

Dựa trên dữ liệu log gốc từ Wazuh, cuộc tấn công diễn ra theo trình tự sau:

- **16:45:33: Giai đoạn 1 - Làm mù hệ thống (Blinding).**
  - Mã độc vô hiệu hóa dịch vụ Windows Defender (WinDefend). Đây là bước đầu tiên để tránh bị phát hiện.
- **17:02:07: Giai đoạn 2 - Cắm chốt (Persistence).**
  - Mã độc ghi đè vào khóa khởi động **Run Key**. Điều này đảm bảo nó sẽ sống sót sau khi khởi động lại máy.
- **17:08:36 - 17:09:07: Giai đoạn 3 - Mở cổng hậu (Backdoor Networking).**
  - Mã độc thực hiện hàng loạt thao tác (Thêm/Xóa) vào cấu hình Windows Firewall (SharedAccess). Mục đích là tạo các quy tắc ngoại lệ để cho phép lưu lượng độc hại đi qua tường lửa.



Mô hình cuộc tấn công khi người dùng kích hoạt virus

IV. PHÂN TÍCH KỸ THUẬT CHI TIẾT

1. PHÂN TÍCH HÀNH VI TẤN CÔNG WINDOWS DEFENDER

Mã độc không chỉ đơn giản là tắt hoặc ngưng dịch vụ mà nó thực hiện 2 kỹ thuật can thiệp sâu vào Registry để ngăn chặn khả năng phục hồi của hệ thống.

1.1. Kỹ thuật: Service Recovery Sabotage (Phá hoại cơ chế phục hồi)

- **Giải thích kỹ thuật:**
  - Trong Windows, mỗi dịch vụ đều có cấu hình **Recovery** (Phục hồi). Nếu dịch vụ bị crash hoặc bị tắt đột ngột, Windows sẽ tự động khởi động lại nó.
  - Mã độc đã chèn thêm giá trị **FailureCommand**. Điều này có nghĩa là: Nếu Windows Defender bị dừng, thay vì khởi động lại nó, hãy chạy một lệnh khác (do virus chỉ định).
  - Đây là kỹ thuật tinh vi để đảm bảo Defender sẽ bị ngắt hoàn toàn và không khởi động trở lại sau khi bị tắt.
- **Bằng chứng:**

```
    "location": "syscheck",
    "decoder": {
      "name": "syscheck_registry_value_added"
    },
    "id": "1769247933.740850",
    "full_log": "Registry Value '[x32]
HKEY_LOCAL_MACHINE\\System\\CurrentControlSet\\Services\\WinDefend\\FailureCommand'
added\nMode: scheduled\n",
    "timestamp": "2026-01-24T09:45:33.558+0000"
  },
  "fields": {
    "timestamp": [
      "2026-01-24T09:45:33.558Z"
```


Log ID 1769247933.740850 xác nhận mã độc đã thêm giá trị FailureCommand vào cấu hình dịch vụ WinDefend. Hành vi này nhằm chiếm quyền điều khiển quy trình khôi phục lỗi, ngăn cản Windows Defender tự khởi động lại.

1.2. Kỹ thuật: ACL Tampering (Can thiệp quyền truy cập)

- **Giải thích kỹ thuật:**
  - Mỗi dịch vụ Windows được bảo vệ bởi một "Security Descriptor" (Mô tả bảo mật), quy định ai (User/Admin/System) có quyền Bật/Tắt dịch vụ.
  - Log cho thấy mã độc đã thay đổi **Kích thước (Size)** và **Mã băm (Checksum)** của key Security.
  - **Mục đích:** Nó ghi đè quyền hạn để tước quyền của Administrator và SYSTEM, khiến cho ngay cả khi bạn là Admin, bạn cũng không thể bật lại Defender được (Access Denied).
- **Bằng chứng:**


```
    "location": "syscheck",
    "decoder": {
      "name": "syscheck_registry_value_modified"
    },
    "id": "1769247933.737258",
    "full_log": "Registry Value '[x32]
HKEY_LOCAL_MACHINE\\System\\CurrentControlSet\\Services\\WinDefend\\Security\\Security'
modified\nMode: scheduled\nChanged attributes: size,md5,sha1,sha256\nSize changed from '244'
to '268'\nOld md5sum was: '2dca7e8c159a70b0f248e2e4e20f7971'\nNew md5sum is :
'9ef374d54e998c23402525c7253da703'\nOld sha1sum was:
'69c8e7fe9b21ac0a421ea981a00249c8f6f34d58'\nNew sha1sum is :
'6f7cb4ee194759b12023a31523276b1e082dc9d6'\nOld sha256sum was:
'0ed00edf0a7a1c727cfbdf9c58bc00e0520bb38f51eca60bd37b90f9007c966f'\nNew sha256sum is :
'1fd2fc1da2bd386144334c8ccc860e571c07081443b925866224bdfda9b4c22d'\n",
    "timestamp": "2026-01-24T09:45:33.551+0000"
```

Log ID 1769247933.737258 cho thấy Security Descriptor của dịch vụ đã bị thay đổi kích thước và nội dung. Đây là dấu hiệu của việc tấn công hạ cấp quyền hạn (Permission Downgrade) hoặc khóa quyền truy cập (Lockout) đối với quản trị viên.

2. PHÂN TÍCH HÀNH VI TẤN CÔNG TƯỜNG LỬA (FIREWALL)

Mã độc thực hiện chiến thuật "Mở cửa hậu" (Backdoor) thông qua việc thao túng các Rule (Luật) trong Registry.

2.1. Kỹ thuật: Rule Injection

- **Giải thích kỹ thuật:**
    - Windows Firewall lưu trữ các luật cho phép/chặn kết nối tại Registry Key FirewallPolicy.
    - Mã độc đã âm thầm chèn một luật mới với định danh GUID lạ: 52a39caa-fbf8-4e0c-8355-ab73852f67c7.
    - Việc chèn trực tiếp vào Registry giúp nó tránh bị phát hiện bởi giao diện người dùng (GUI) thông thường.
- **Bằng chứng:**

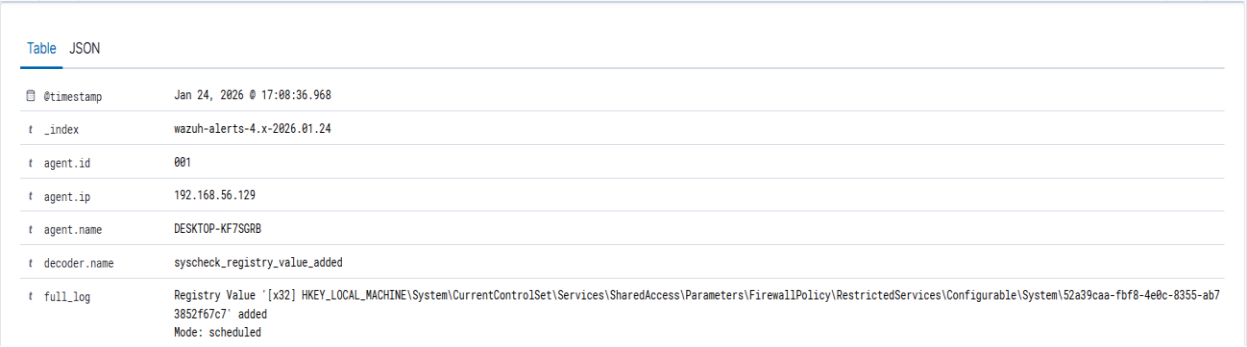


Table JSON

@timestamp	Jan 24, 2026 @ 17:08:36.968
_index	wazuh-alerts-4.x-2026.01.24
agent.id	001
agent.ip	192.168.56.129
agent.name	DESKTOP-KF7SGRB
decoder.name	syscheck_registry_value_added
full_log	Registry Value '[x32] HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\RestrictedServices\Configurable\System\52a39caa-fbf8-4e0c-8355-ab73852f67c7' added Mode: scheduled

Log ID 1769249316.780058 ghi nhận một quy tắc tường lửa mới được thêm vào với định danh GUID 52a39caa.... Quy tắc này hoạt động như một giấy phép thông hành, cho phép mã độc kết nối ra máy chủ điều khiển (C2) mà không bị tường lửa chặn.

2.2. Kỹ thuật: Security Disarmament

- **Giải thích kỹ thuật:**

- Ngay sau khi thêm luật của mình, mã độc thực hiện hành vi xóa (deleted) một luật khác có GUID {7A0BBEFE...}.
- Đây có thể là hành vi xóa luật chặn mặc định của Windows, hoặc xóa dấu vết của chính nó sau khi đã thiết lập xong kết nối (Cleanup).

- **Bằng chứng:**

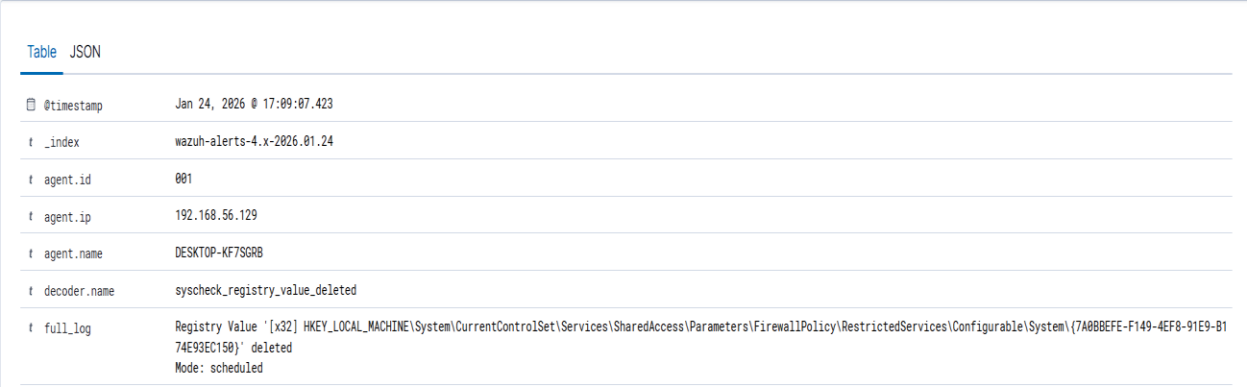


Table JSON

@timestamp	Jan 24, 2026 @ 17:09:07.423
_index	wazuh-alerts-4.x-2026.01.24
agent.id	001
agent.ip	192.168.56.129
agent.name	DESKTOP-KF7SGRB
decoder.name	syscheck_registry_value_deleted
full_log	Registry Value '[x32] HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\RestrictedServices\Configurable\System\{7A0BBEFE-F149-4EF8-91E9-B174E93EC150}' deleted Mode: scheduled

Log ID 1769249347.790880 xác nhận hành vi xóa bỏ cấu hình tường lửa hiện có. Việc xóa Registry Key này làm suy yếu lớp bảo vệ mạng của hệ điều hành.

V. KẾT LUẬN

Hệ thống phòng thủ của máy **DESKTOP-KF7SGRB** đã bị thất thủ hoàn toàn:

1. **Windows Defender:** Đã bị tắt.
2. **Tường lửa:** Đã bị vô hiệu hóa (SharedAccess).
3. **Hiện trạng:** Máy tính đang nằm dưới sự kiểm soát của kẻ tấn công thông qua cơ chế **Persistence**.