**aCẢNH BÁO LỖ HỔNG**

**Ngày 21 tháng 10, 2023**

**Mô tả**

Báo cáo mô tả quá trình và kết quả kiểm thử ứng dụng CMC Antivirus

**Đối tượng**

CMC Antivirus version v1.1.2022 build 117, Revision 131577

**Thành viên thực hiện**

Nông Hoàng Tú

**Công cụ**: arpspoof, dns\_spoof.py, metasploit-framework, VMware Workstation, vi, zip, apache2, zipinfo

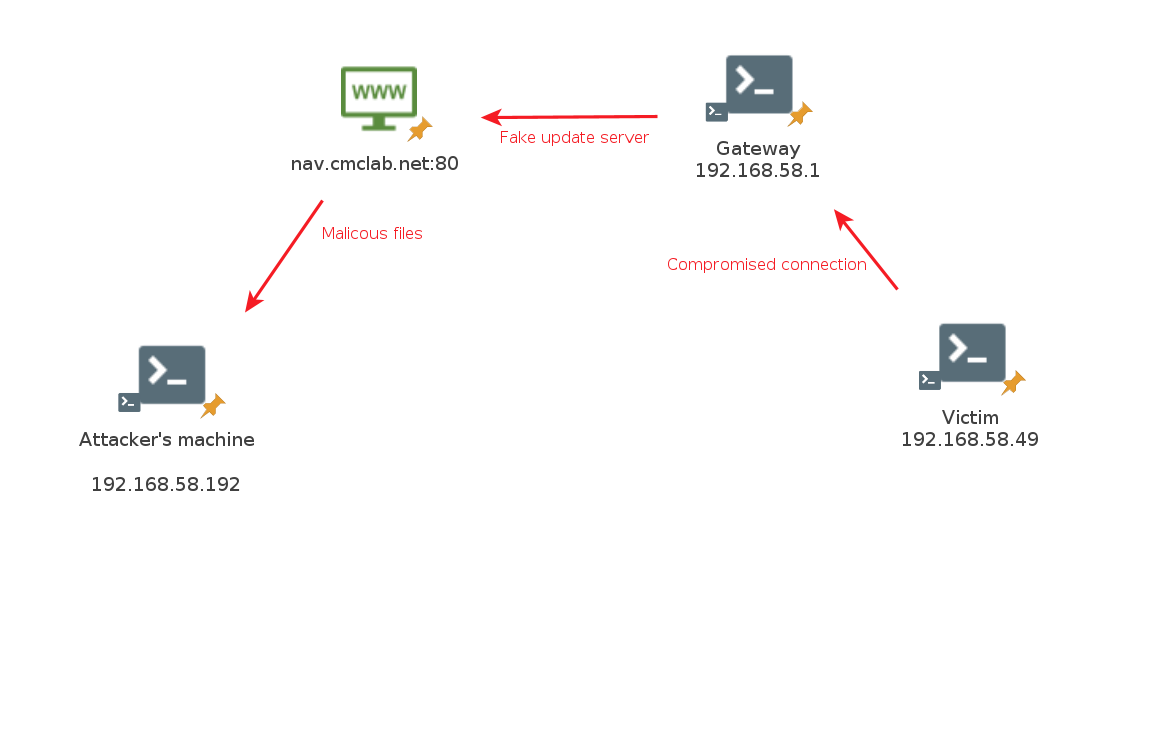
WSTG-CRYP-01: Server nav.cmclab.net không sử dụng kết nối có mã dẫn tới người dùng bị tấn công bởi server giả mạo [High]

Description and impact

CMC Antivirus tiến hành cập nhật phiên bản mới thông qua giao thức HTTP. Qua phân tích, tôi phát hiện CMC Antivirus kết nối tới URL <http://nav.cmclab.net> là một giao thức không có mã hóa. Vì vậy, attacker có thể sử dụng kỹ thuật DNS Spoofing để giả mạo update server, khiến người dùng tải về bản cập nhật giả mạo có chứa file độc hại.

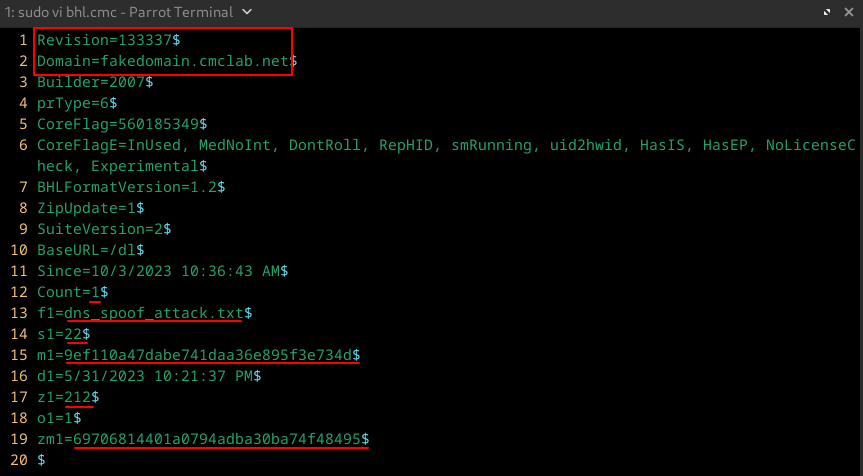
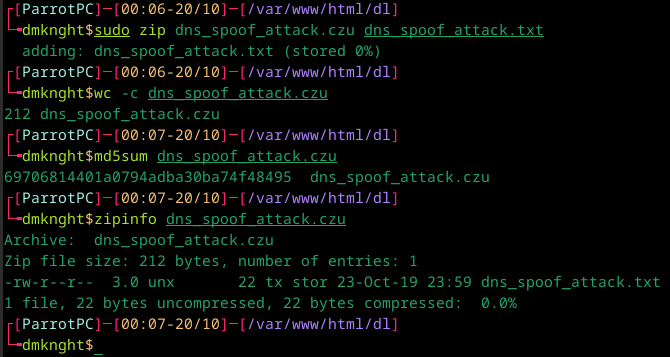
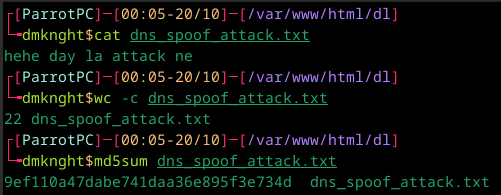
Steps to reprocedure

Quá trình tấn công sử dụng mô hình mạng được mô tả như hình bên dưới

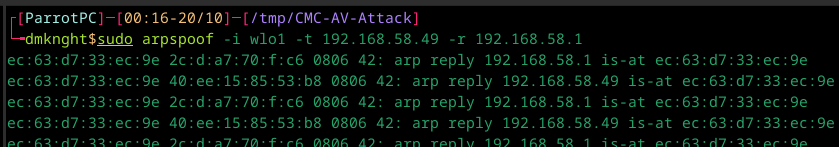


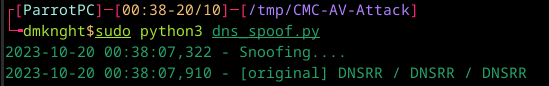
Attacker tiến hành tạo các file update giả mạo. Các file này có kiến trúc giống với file trên server nên CMC Antivirus hiểu nhầm là các file hợp lệ. Các file bao gồm:

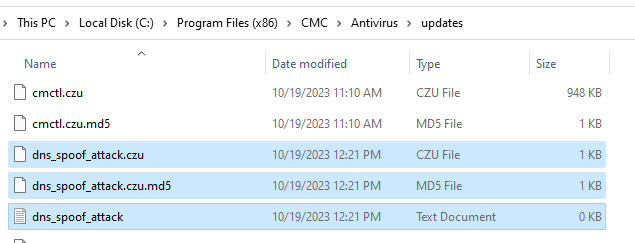
1. dns\_spoof\_attack.txt tại thư mục dl nằm trong DocumentRoot. File này đóng vai trò file update giả mạo
2. dns\_spoof\_attack.czu nằm trong thư mục dl. Đây là file nén dạng zip của dns\_spoof\_attack.txt
3. bhl.cmc tại thư mục cu nằm trong DocumentRoot. Đây là file Index được CMC Antivirus đọc nhằm kiểm tra các file có update mới cần tải xuống.



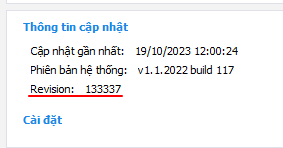
Tiếp theo, attacker tiến hành tấn công ARP Spoofing và DNS Spoofing nhằm chuyển hướng kết nối tới server attacker tạo ra.





Tại phía người dùng, kết nối tới domain nav.cmclab.net đã bị redirect sang server giả mạo của attacker. CMC Antivirus đã tải về file giả mạo trong thư mục updates.

Thông tin phiên bản cho thấy CMC AV đã thay đổi giá trị version thành giá trị mà attacker setup.



References

* Công cụ sử dụng để tấn công DNS Spoofing: <https://www.geeksforgeeks.org/how-to-make-a-dns-spoof-attack-using-scapy-in-python/>

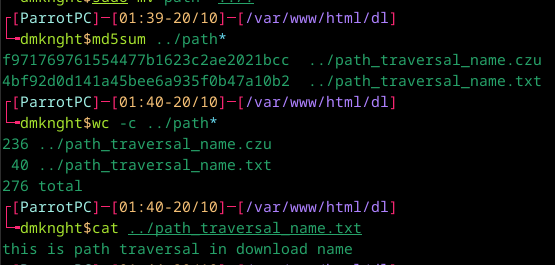
WSTG-ATHZ-01: Path traversal trong file name dẫn tới ghi file ngoài thư mục update [Low]

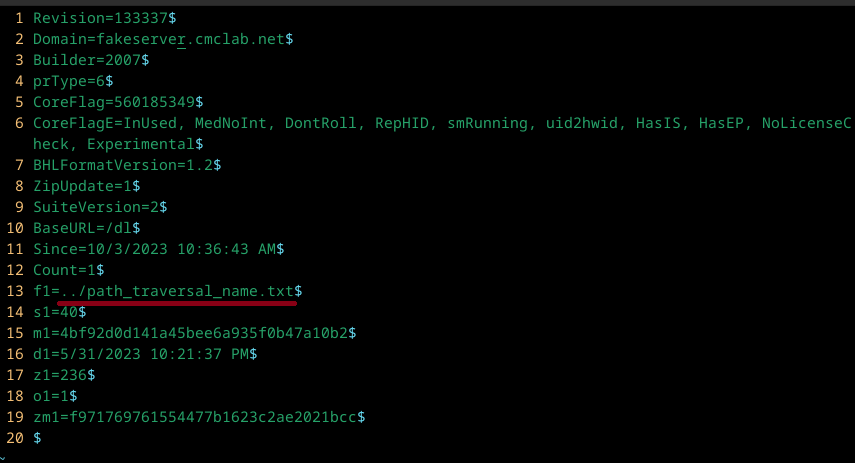
Description and impact

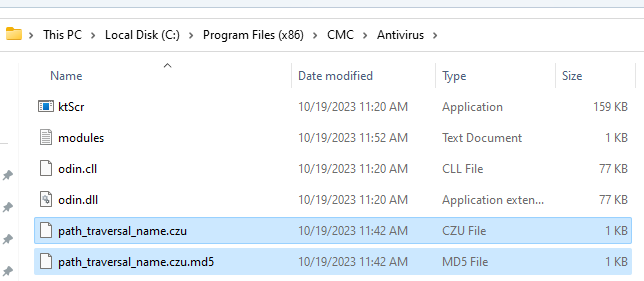
Chức năng update của CMC Antivirus sử dụng tên nằm trong bhl.cmc để xử lý quá trình tải file. Tôi đã phát hiện lỗ hổng path traversal của chức năng này dẫn đến CMC Antivirus ghi file .czu và .md5 vào vị trí bất kỳ trong hệ thống.

Steps to reprocedure

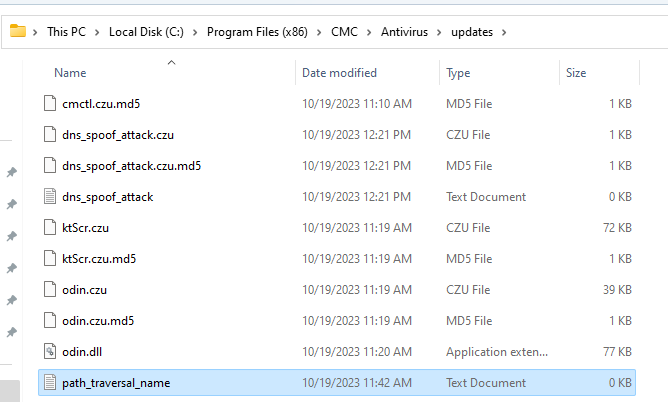
Attacker tiến hành tạo file update giả mạo với giá trị file name có chứa relative path là ../



CMC Antivirus tiến hành cập nhật phiên bản mới. Các file .czu và .md5 được ghi ra ngoài thư mục updates.



Trong khi đó, nội dung file .czu được giải nén đã được ghi vào trong thư mục updates



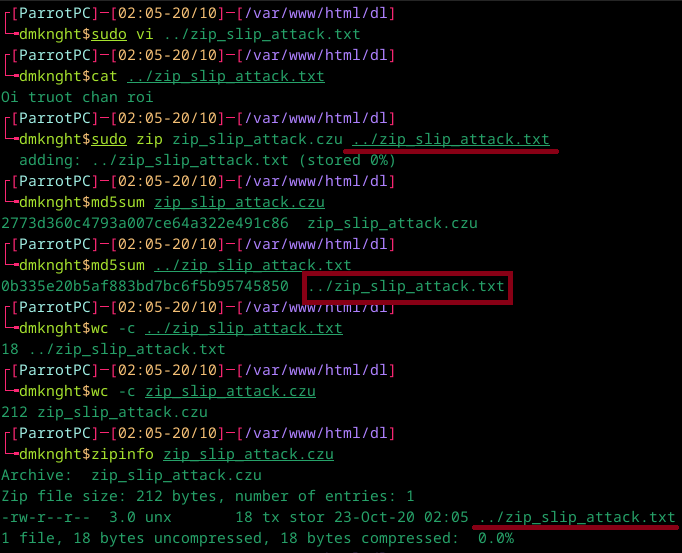
WSTG-ATHZ-01: Lỗ hổng path traversal trong quá trình giải nén dẫn tới ghi file vào vị trí bất kỳ trong hệ thống [High]

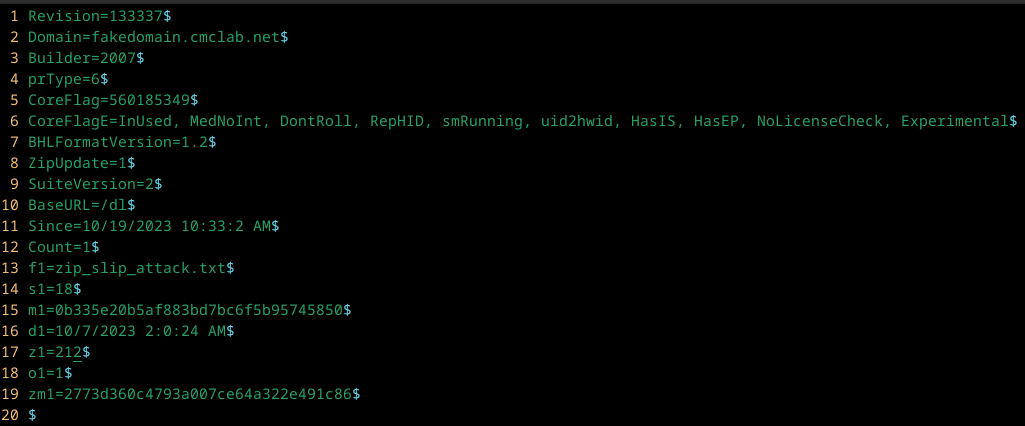
Description and impact

Quá trình update của CMC Antivirus tiến hành giải nén dữ liệu trong file .czu. Tại đây, tôi phát hiện lỗ hổng path traversal dẫn tới file được nén trong file .czu có thể được ghi vào bất kỳ đâu trong hệ thống.

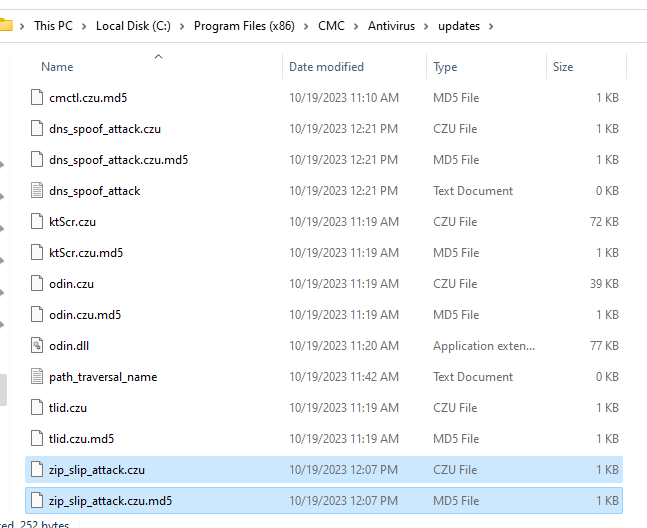
Steps to reprocedure

Attacker tiến hành tạo file giả mạo mà đường dẫn có chứa ../ rồi tiến hành nén zip

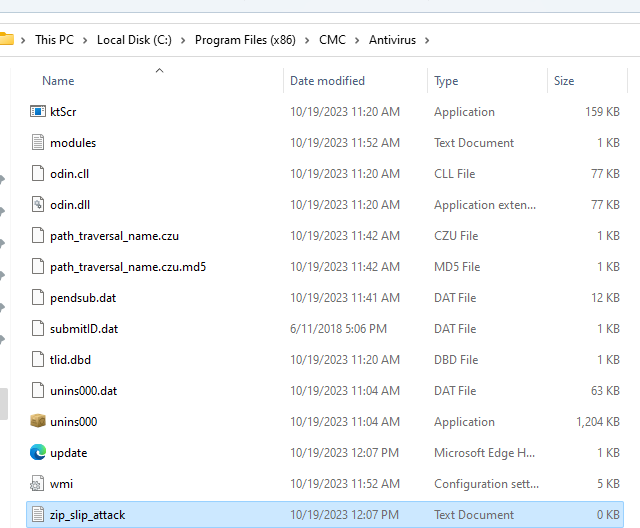




CMC AV tiến hành cập nhật và tải file về. File .czu và .md5 được ghi vào trong thư mục updates.



Trong khi đó, file được giải nén ra đã được ghi vào thư mục nằm ngoài thư mục updates



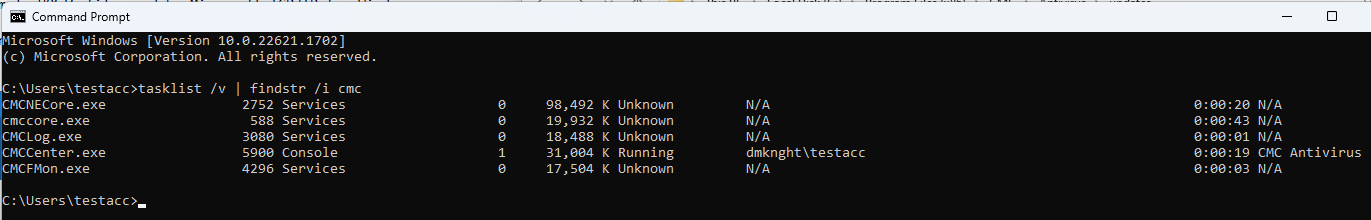
Khai thác lỗ hổng path traversal trong quá trình giải nén để chiếm quyền điều khiển hệ thống từ xa [High]

Description and impact

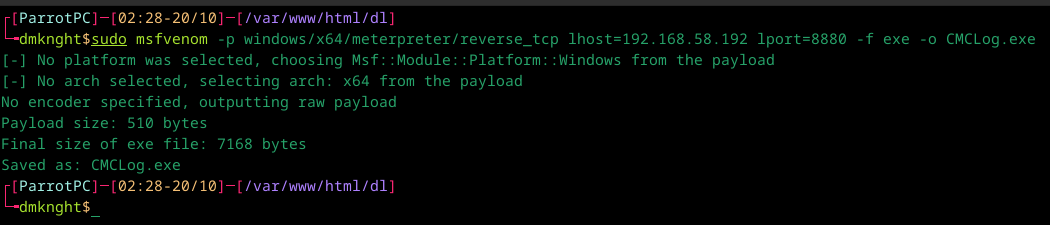
Attacker lợi dụng lỗ hổng path traversal trong quá trình giải nén file zip để ghi đè file mã độc vào file của CMC. Thông qua quá trình này, attacker có thể chiếm quyền điều khiển máy tính nạn nhân sau khi nạn nhân reboot máy. Mã độc được thực thi có quyền cao nhất trong hệ thống và được CMC self-defense bảo vệ.

Step to reprocedure

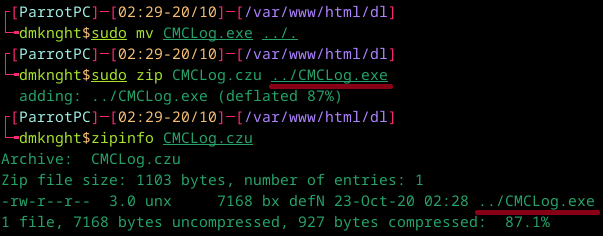
Công cụ tasklist của Windows cho thấy CMC Antivirus khởi chạy một số dịch vụ với quyền SYSTEM. Những dịch vụ này có thể được attacker lợi dụng để ghi đè mã độc. File CMCLog.exe được lựa chọn.

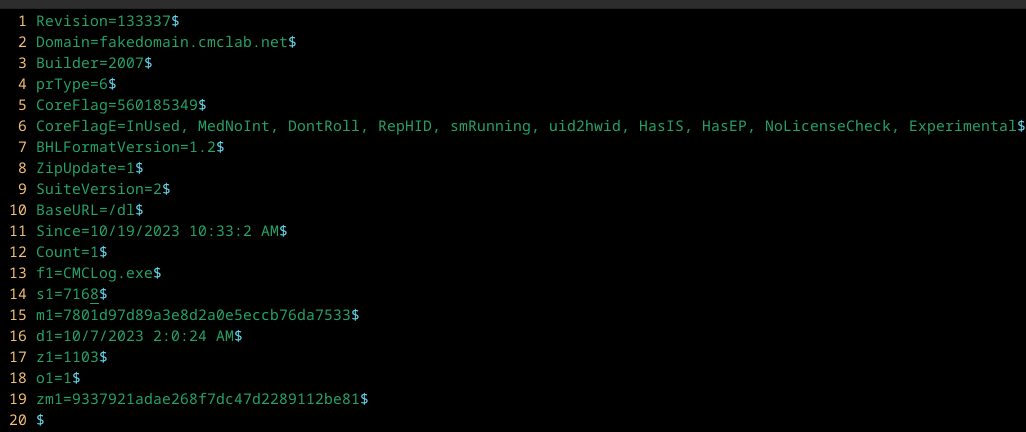


Đầu tiên, attacker tạo backdoor với công cụ msfvenom với tên CMCLog.exe



Tiếp theo, attacker tiếp tục tạo file trên server nhằm khai thác lỗ hổng path traversal như đã mô tả ở trên.

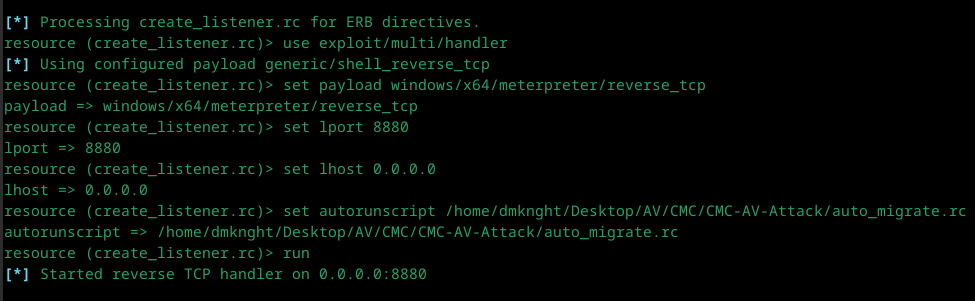


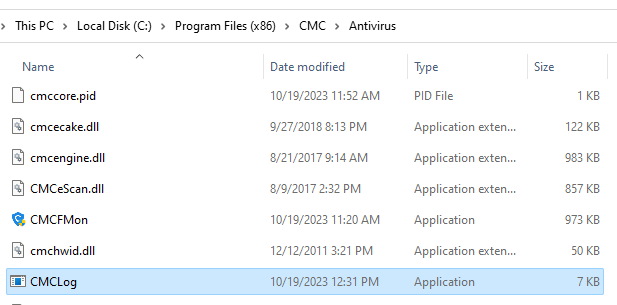


Attacker tiến hành tạo listener tự động migrate backdoor vào tiến trình lsass.exe ngay khi kết nối được thiết lập.





Khi victim tiến hành cập nhật. File CMCLog.exe đã bị ghi đè bởi file mã độc mà attacker tạo ra.



Sau khi victim khởi động lại máy, mã độc được kích hoạt và attacker chiếm quyền điều khiển hệ thống với quyền cao nhất

