claimAV

viết tài liệu các tool inject code

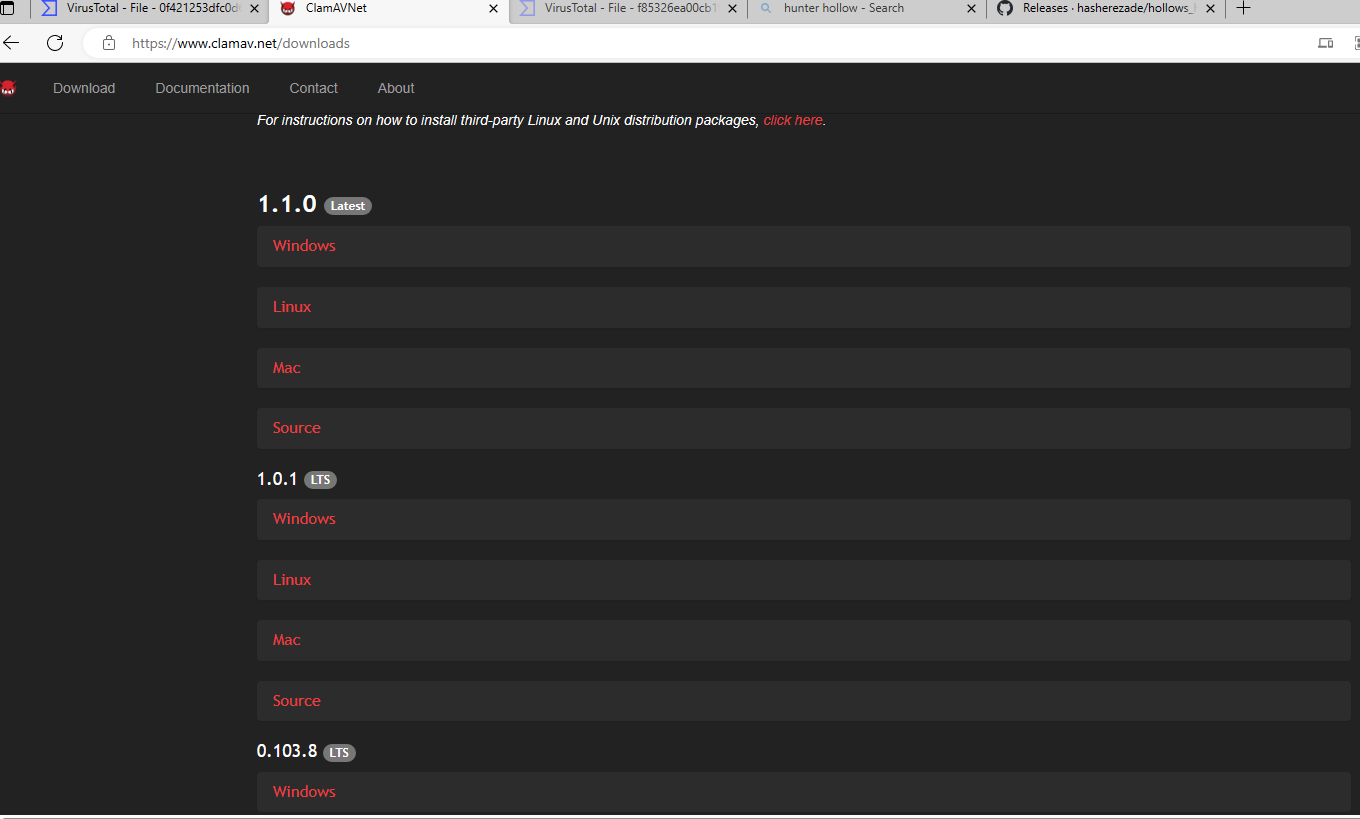
tìm hiểu cơ chế viết luật trong sysmon

triển khai kịch bản từ quá trình inject code vào hidden process và phát hiện với sysmon

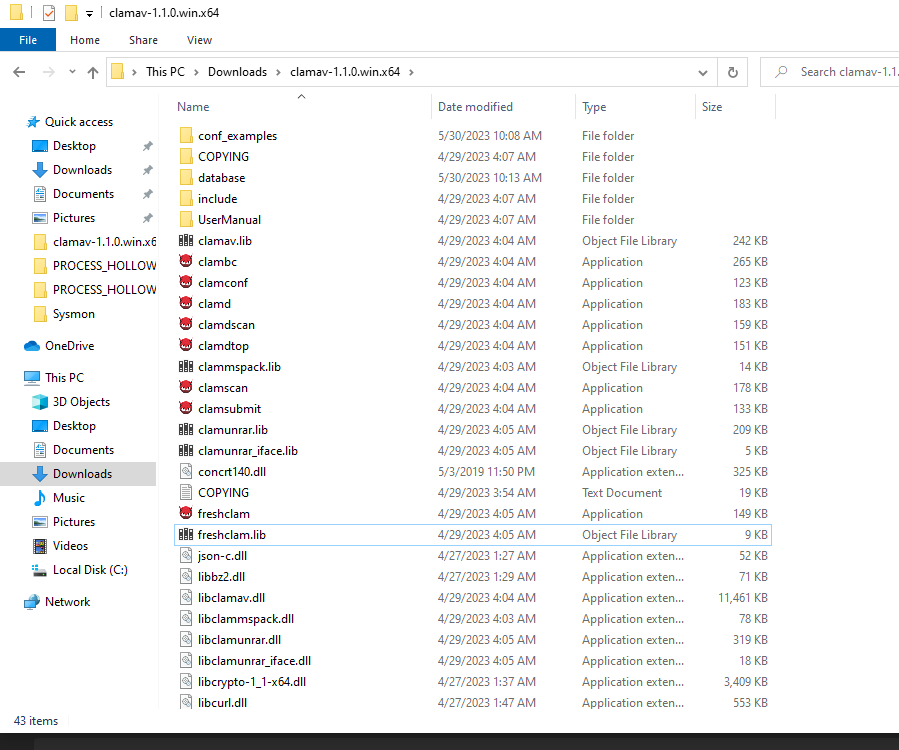
triển khai kịch bản tương tự với dll exe phát hiện bằng clamAV

Cài đặt và sử dụng calmAV

Truy cập <https://www.clamav.net/downloads> để tải ClamAV. Lựa chọn phiên bản thích hợp với hệ điều hành

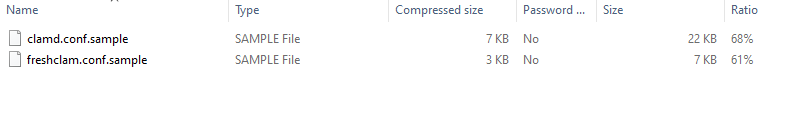


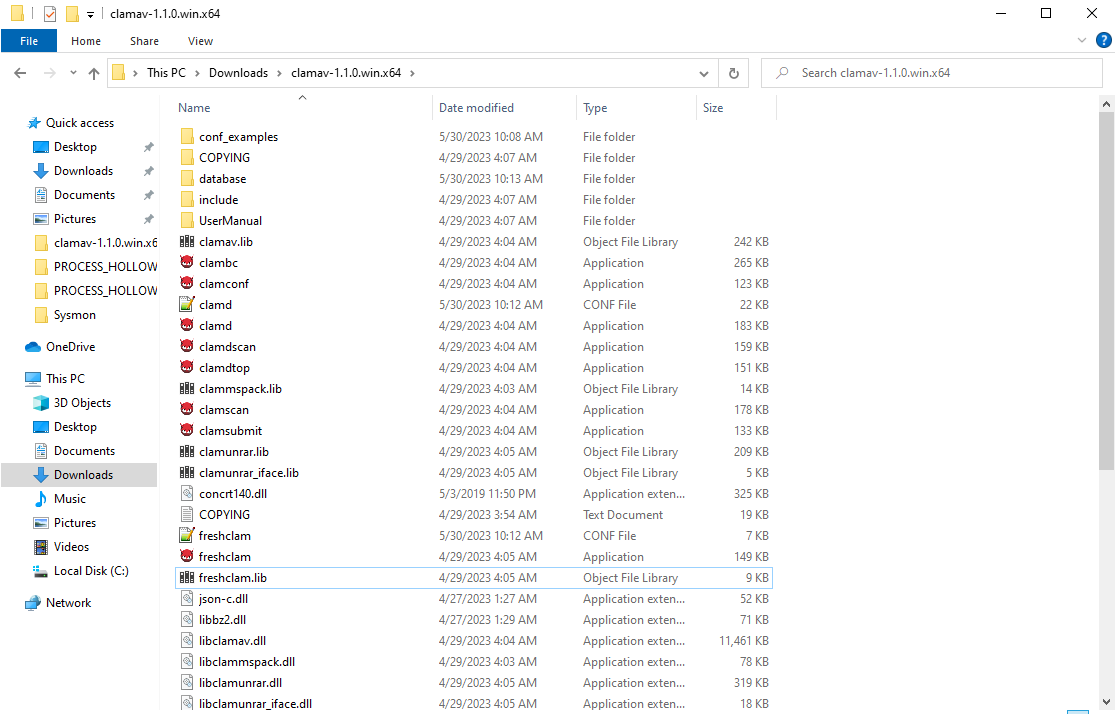
Tải về và giải nén



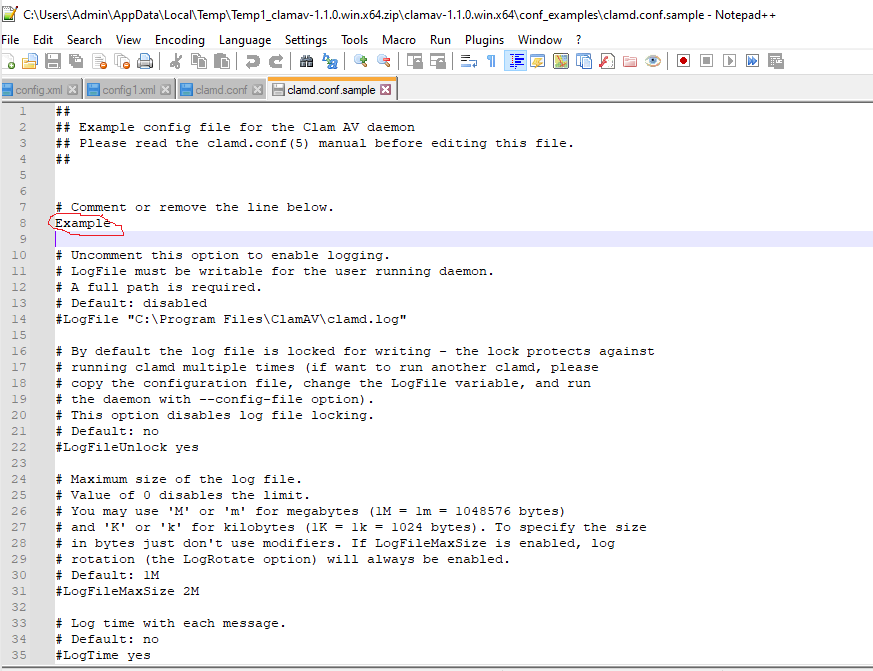
Vào thư mục conf\_example xóa đuôi .sample trong 2 file clamd.conf và freshclam.conf

Di chuyển 2 file này ra ngoài

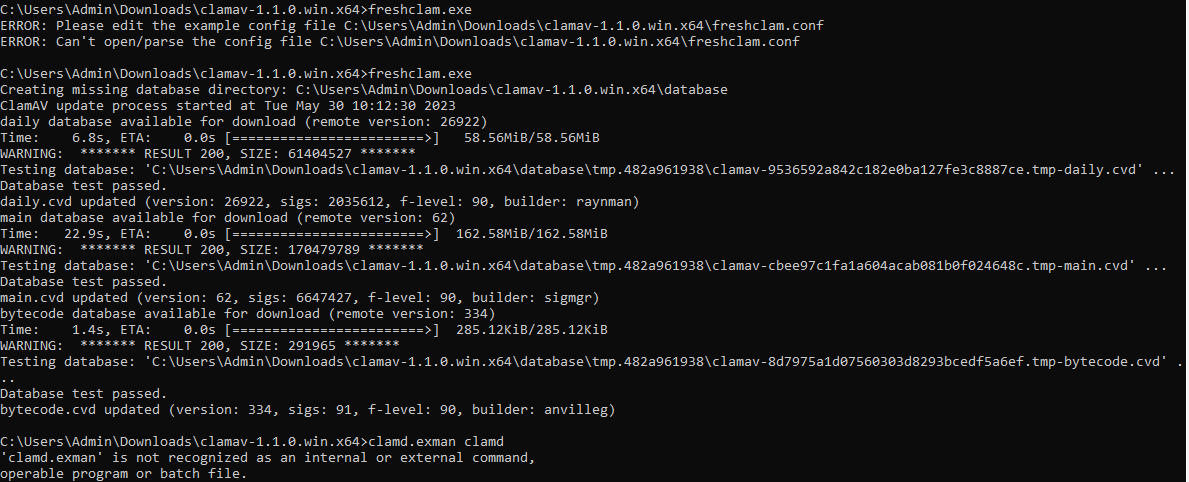




Vào 2 file .conf này và xóa dòng example

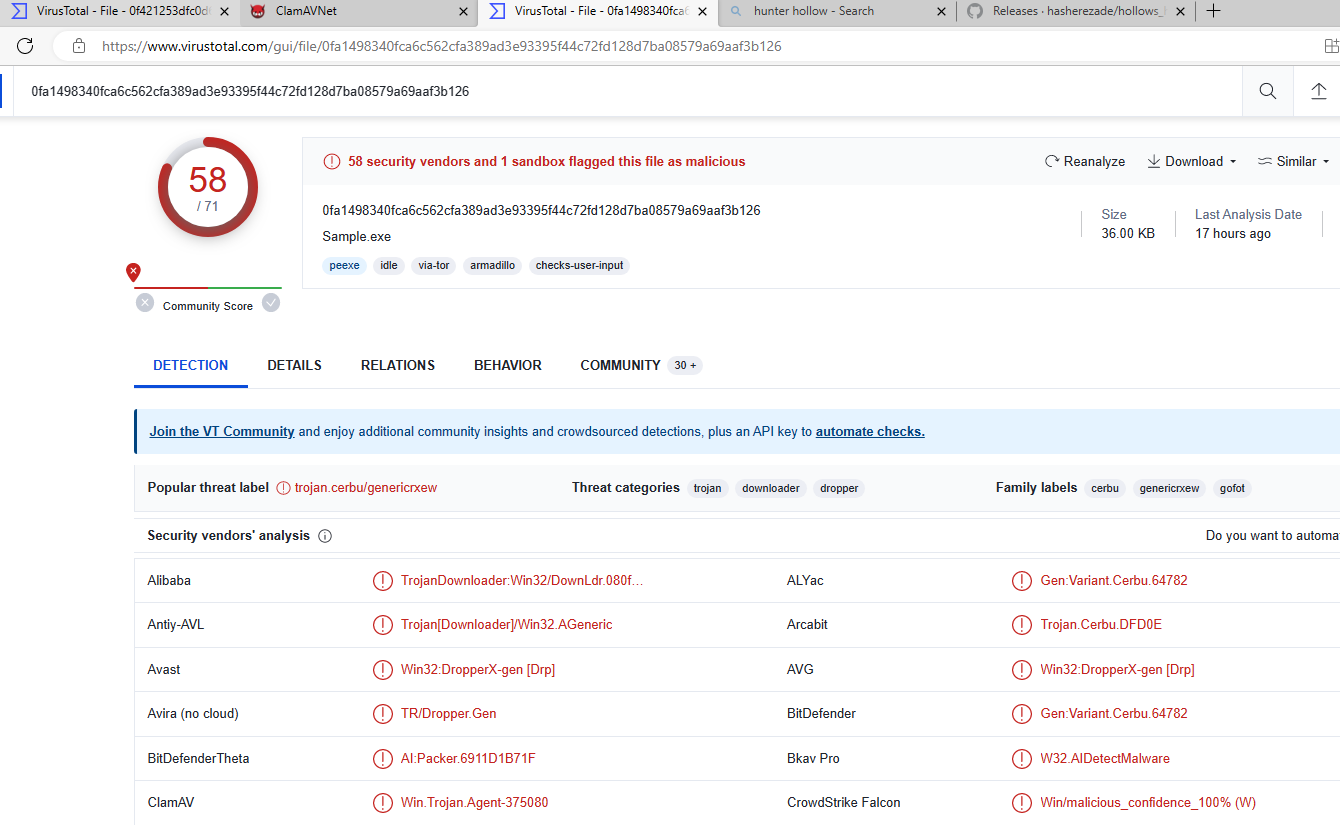


Nhập freshclam.exe để cập nhật cơ sở dữ liệu

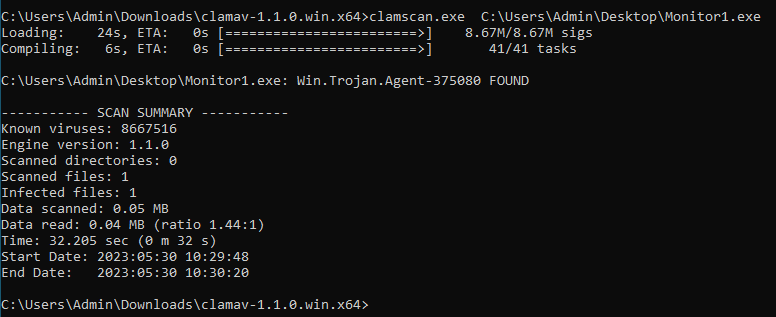


Các bước chuẩn bị đã xong tiến hành quét mã độc bằng clamAV

Với file mã độc monitor1.exe đưa lên virus total tỉ lệ nhận diện mã độc rất cao



Scan 1 file bằng clamAV



ClamAV dựa trên signatures để phân biệt file sạch và file độc hại

* File hash signatures
* Bytecode signatures
* Phishing Signatures

**Ngoài ra clamAV còn có thể xử lý các Yara rule**

Yara rule cho phép tạo ra các quy tắc để phát hiện mã độc dựa trên các đặc điểm. mỗi quy tắc gồm tập hợp các chuỗi, địa chỉ , hàm import , ioc, hàm băm, … kết hợp với các điều kiện logic để phát hiện mã độc

Ưu điểm của yara rule so với signature-base

* Có tính linh hoạt hơn
* Các rule được xây dựng dưới dạng ngôn ngữ lập trình giúp dễ dàng xây dựng và phát triển
* Có thể phát hiện dựa trên hành vi, phân tích bộ nhớ

https://yara.readthedocs.io/en/stable/writingrules.html

<https://github.com/Yara-Rules/rules>

<https://github.com/mikesxrs/Open-Source-YARA-rules/blob/master/h3x2b/injection.yara>