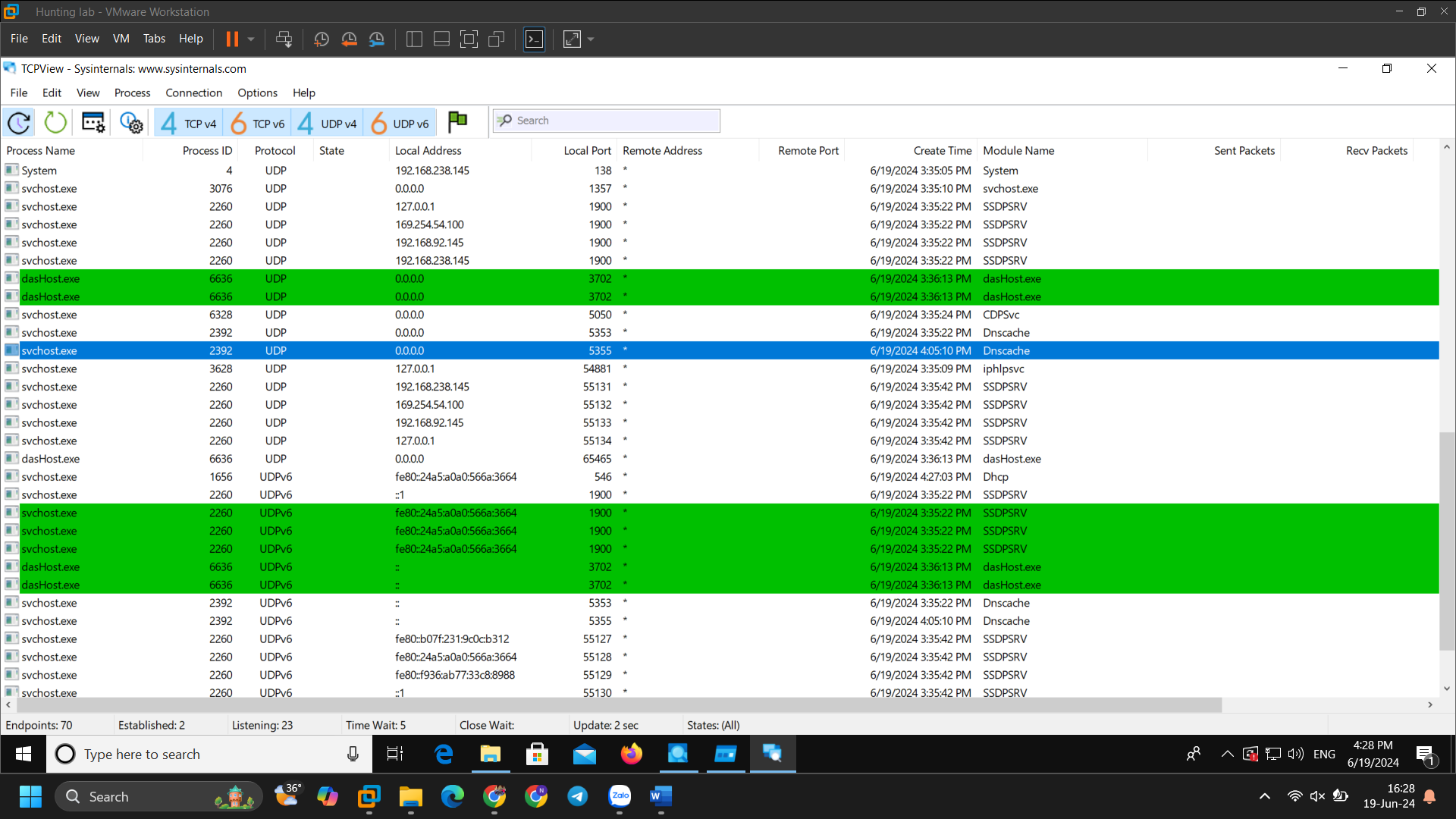
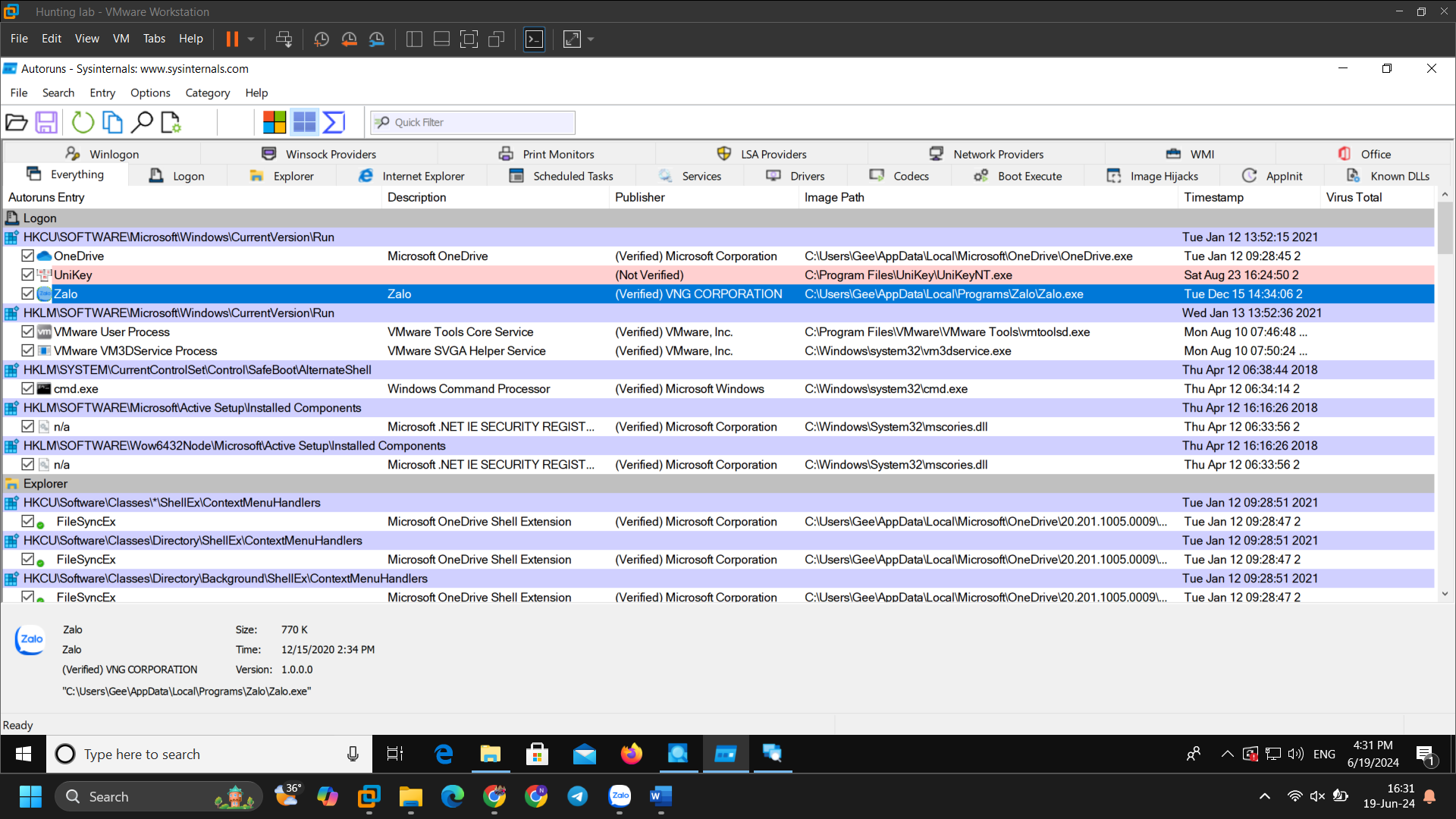
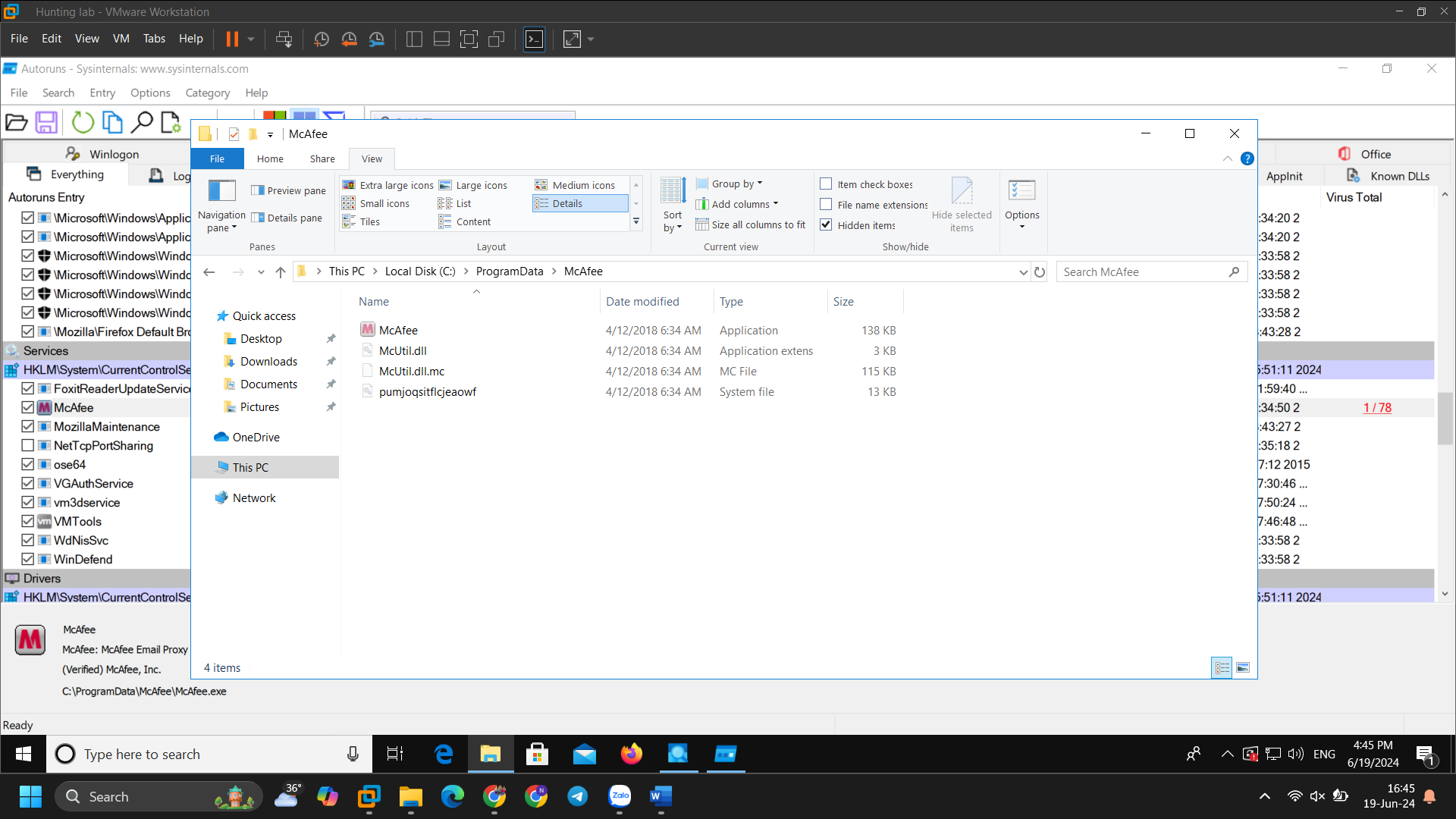
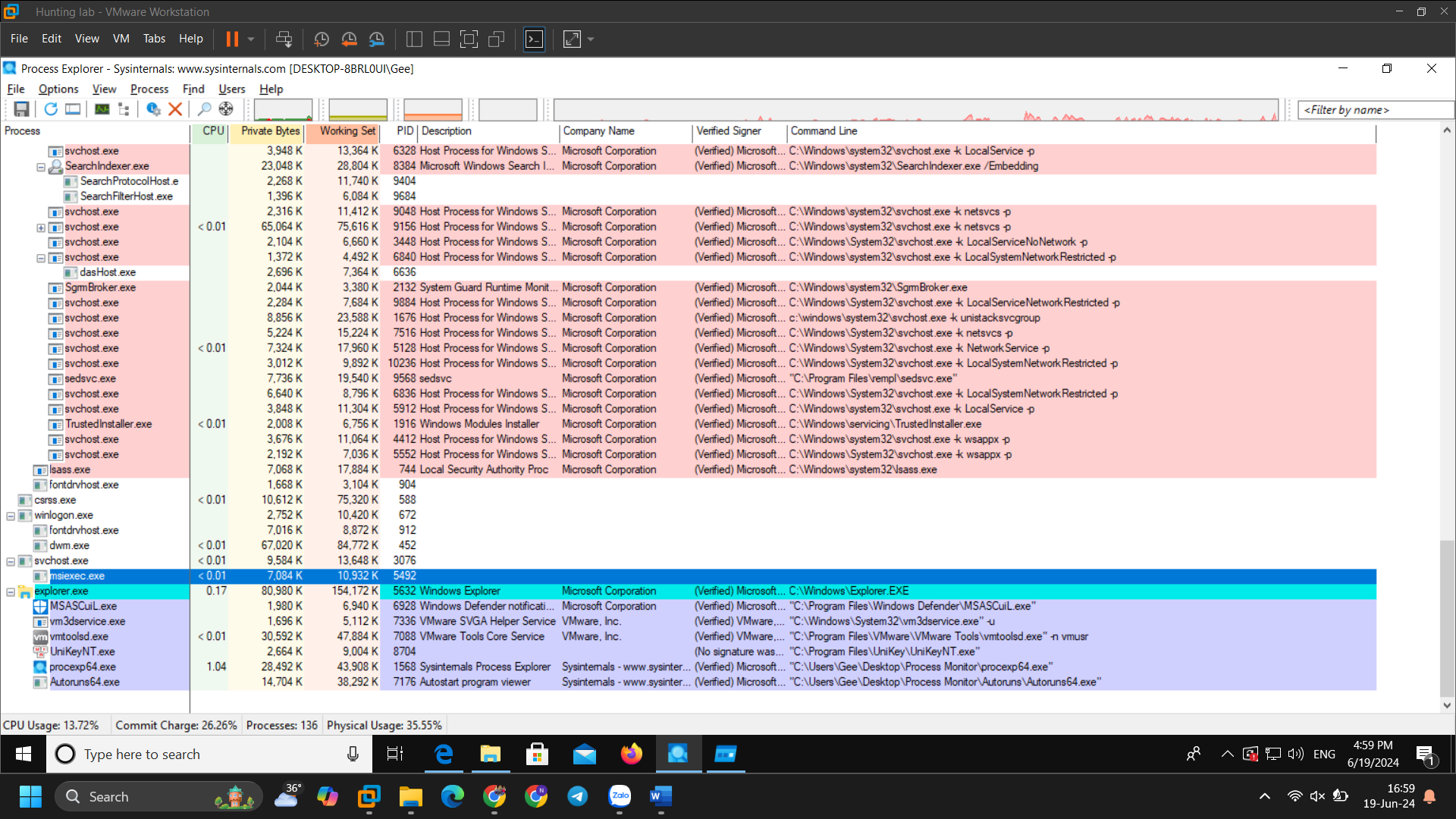
Windows Hunting Lab - Đi tìm mã độc trong Windows (8).  
https://drive.google.com/file/d/1aktTX61sVduXjNY7735yPgfZkWWF\_XEF/view?usp=sharing

Kiểm tra Network TCPView: Tự máy gọi đến chính máy đó. Không có gì bất thường.  


Kiểm tra Autoruns: Xem CMD hay Explorer có chạy thêm những file nào khác không, xem các file dll. Ngoài ra xem cả đường dẫn của các file đó (ví dụ các file thực thi thuộc về Program Files, Program Files x86).  


* Kiểm tra CMD: Không có dấu hiệu bất thường.
* Kiểm tra OneDrive: Đã được ký, không có dấu hiệu bất thường.
* Kiểm tra Unikey: Chưa được ký do không có tiền cho nên Autoruns đã đánh dấu, giống như attacker sẽ theo dõi hành vi của người dùng trên bàn phím, cho nên được hiển thị đỏ. Tuy nhiên Unikey không có dấu hiệu có mã độc.
* Kiểm tra Zalo: Đã được ký, không có dấu hiệu bất thường.
* Kiểm tra NppShell và WinRAR: Không có dấu hiệu bất thường.
* Kiểm tra McAfee: Đã được ký nên khả năng sẽ không có dấu hiệu bất thường. Tuy nhiên, trong C:\ProgramData\McAfee lại không hiển thị thư mục nào nên khả năng McAfee là 1 file bị ẩn. Phải sử dụng show hidden files. Ở đây kẻ tấn công sẽ sideload và fake thư mục McAfee. Từ đó có thể suy ra McAfee với McUtil.dll là mã độc.  
  
* Khi nào tiến trình mã độc trong ControlSetService này được chạy: Khi khởi động hệ thống và các service này sẽ được chạy.

Kiểm tra Process Explorer: Xem các tiến trình con và tiến trình cha.  


* Msiexec.exe được chạy ở dưới svchost.exe. Khi chạy McAfee lên thì nó là service từ winlogon.exe, McAfee sẽ load file McUtil.dll. Khi McUtil.dll được chạy thì sẽ gọi các trình động. Tuy nhiên McUtil.dll không được ra output như mong muốn nên svchost.exe bị chạy ra ngoài winlogon.exe.
* Xác định các file mã độc, suspend mã độc và xóa mã độc trong File Explorer. Cuối cùng thì gỡ msiexec.exe và svchost.exe.

Tool để quét tất cả tiến trình: hollows\_hunter.  
Tool để quét một tiến trình: pe-sieve.