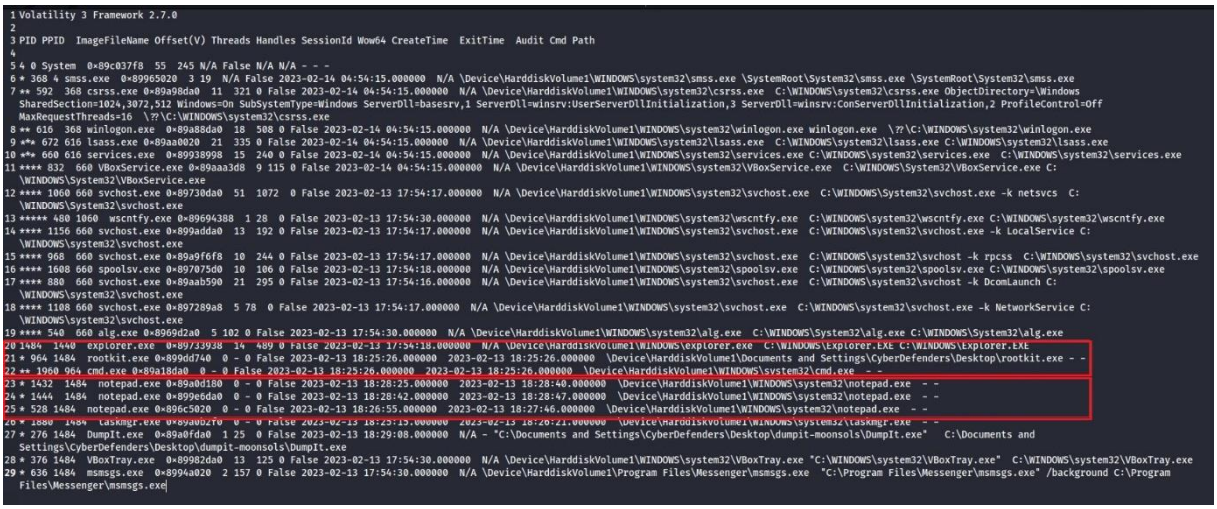
Bu çalışmada BlackEnergy zararlı yazılımı tarafından enfekte edilmiş bir sistemin alınan ram imajı analiz edilecektir.

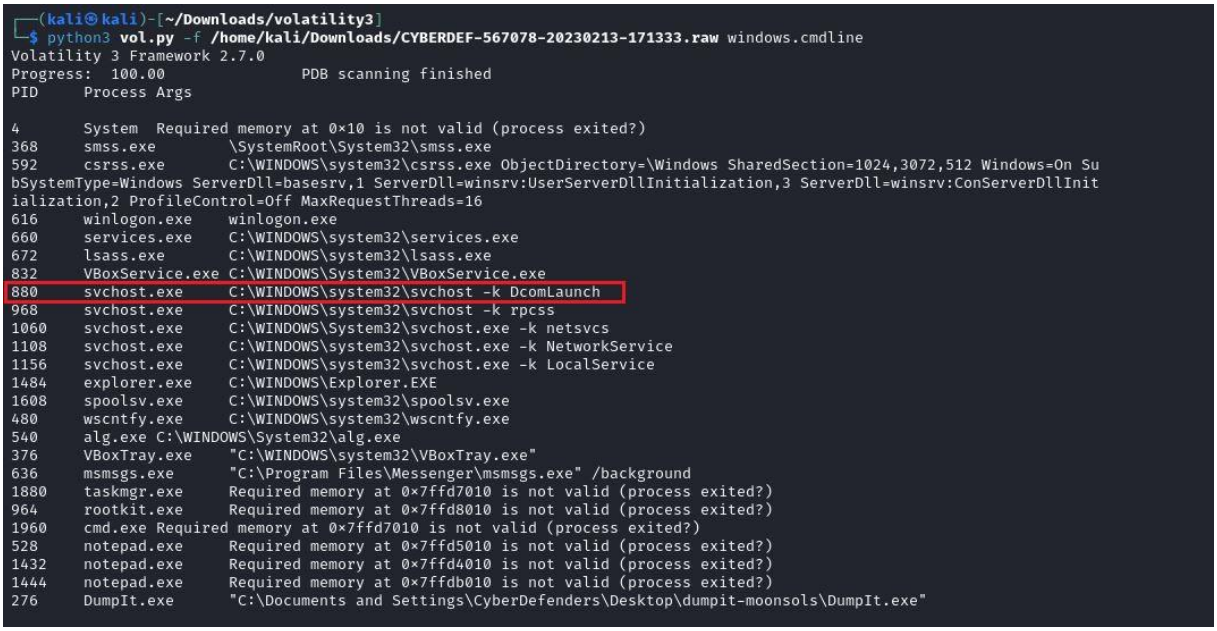
İmaj alınırken sistemde çalışan processlerin neler olduğunu görmek için Windows.pstree komutunu kullanacağız. Bu komut ile çalışan processlerin parent-child ilişkilerini inceleyeceğiz. Bunun için aşağıdaki komutu çalıştırıyoruz.



python3 vol.py -f /home/kali/Downloads/CYBERDEF-567078-20230213-171333.raw windows.pstree

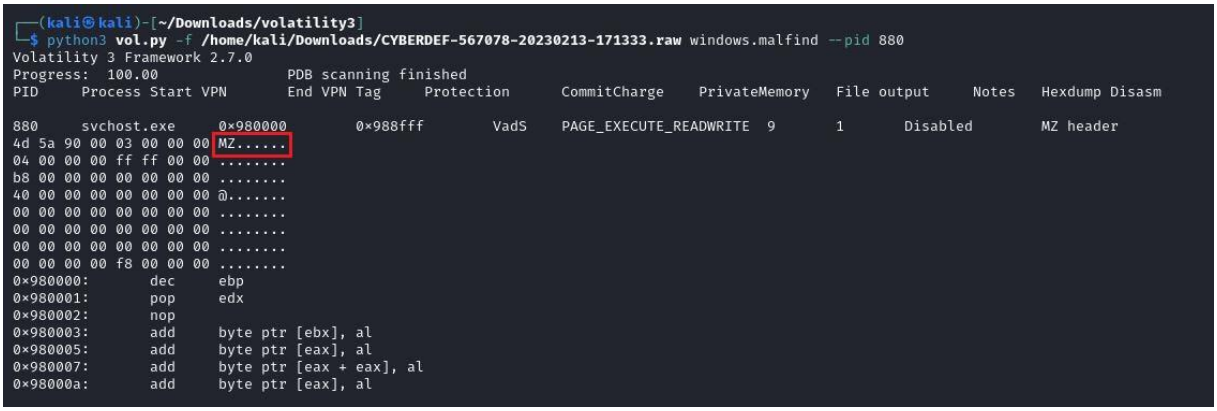
Bu çıktıda explorer.exe tarafından oluşturulan, rootkit.exe ve cmd.exe arasındaki ilişki şüphe uyandırıcı. Aynı zamanda yine explorer.exe tarafından oluşturulan notepad.exe süreçleri de şüphe uyandırıcı. Tüm bunlar akla dll injection saldırısını getiriyor.

Burada windows.cmdline komutunu çalıştırarak süreçlere ait komut satırı argümanlarını inceleyelim.



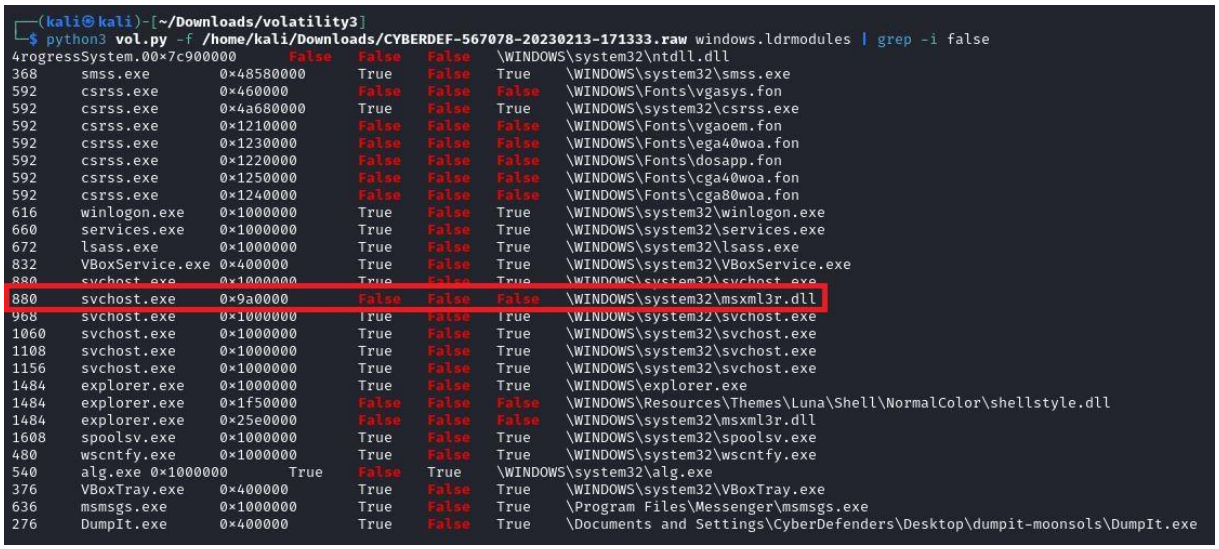
python3 vol.py -f /home/kali/Downloads/CYBERDEF-567078-20230213-171333.raw windows.cmdline

Bazen kötü amaçlı yazılımlar, kötü amaçlı kod enjekte etmek veya sistemde yetkisiz eylemler gerçekleştirmek için svchost.exe -k DcomLaunch sistem işlemini kullanır. Yukarıdaki çıktıda pid değeri 880 olan svchost.exe süreci bu amaç için çalışıyor olabilir. Bu sebeple svchost.exe için windows.malfind aracını çalıştırarak olası bir injection saldırı durumu var mı inceleyelim.



python3 vol.py -f /home/kali/Downloads/CYBERDEF-567078-20230213-171333.raw windows.malfind --pid 880

Görünüşe göre bu svchost.exe dosyası sistem tarafından oluşturulmamış. O halde bu dosya svchost.exe 'nin adını kullanan bir zararlı yazılım olabilir. Bu aşamada Windows.ldrmodules aracını kullanarak gizlenmiş dll dosyalarını tespit etmeye çalışalım.



python3 vol.py -f /home/kali/Downloads/CYBERDEF-567078-20230213-171333.raw windows.ldrmodules | grep -i false

msxml3r.dll dosyasının bağlantıları kesilmiş, o halde msxml3r.dll dosyası gizlenmiş olabilir.