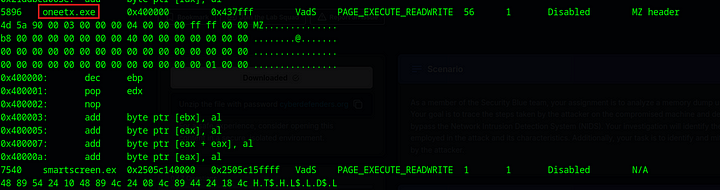
### **RedLine Lab — CyberDefenders**

**Scenario:** As a member of the Security Blue team, your assignment is to analyze a memory dump using Redline and Volatility tools. Your goal is to trace the steps taken by the attacker on the compromised machine and determine how they managed to bypass the Network Intrusion Detection System (NIDS). Your investigation will identify the specific malware family employed in the attack and its characteristics. Additionally, your task is to identify and mitigate any traces or footprints left by the attacker.

**1.What is the name of the suspicious process?**

Lists process memory ranges that potentially contain  
 injected code.

vol.py -f MemoryDump.mem windows.malfind



Oneetx.exe looks suspicious. Let us examine the process relation of this process.



It launches rundll32.exe, which is commonly exploited by LOLBINS.

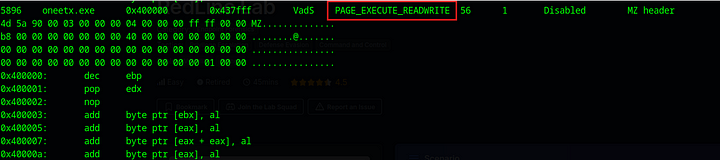
**Answer:** Oneetx.exe

**2. What is the child process name of the suspicious process?**

**Answer:** rundll32.exe

**3. What is the memory protection applied to the suspicious process memory region?**

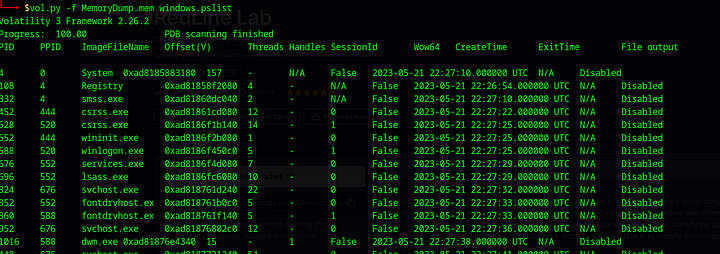
We can see this in the malfind output.



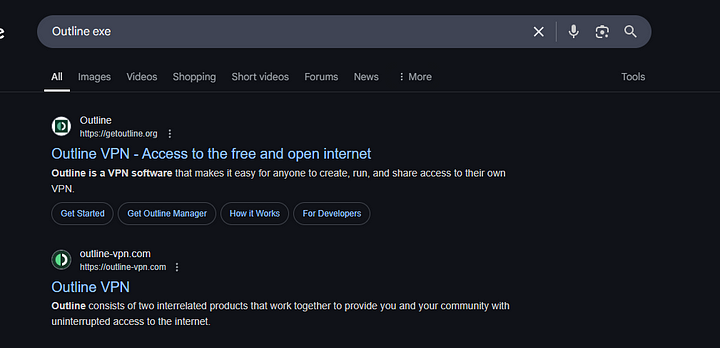
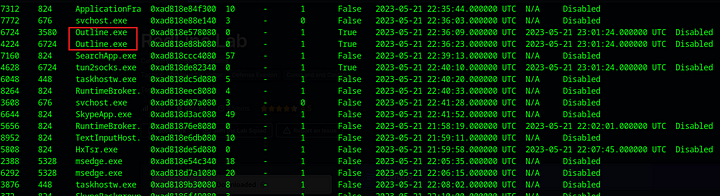
**Answer:** PAGE\_EXECUTE\_READWRITE

**4. What is the name of the process responsible for the VPN connection?**

vol.py -f MemoryDump.mem windows.pslist



While searching for the processes I dont recognize, I found that one of these processes is a VPN.

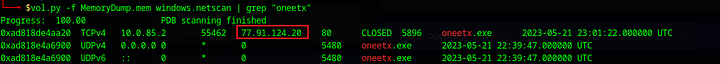


**Answer:** Outline.exe

**5. What is the attacker’s IP address?**

Let us use the netscan plugin to see which IP address did the suspicious process contact.

vol.py -f MemoryDump.mem windows.netscan | grep "oneetx"

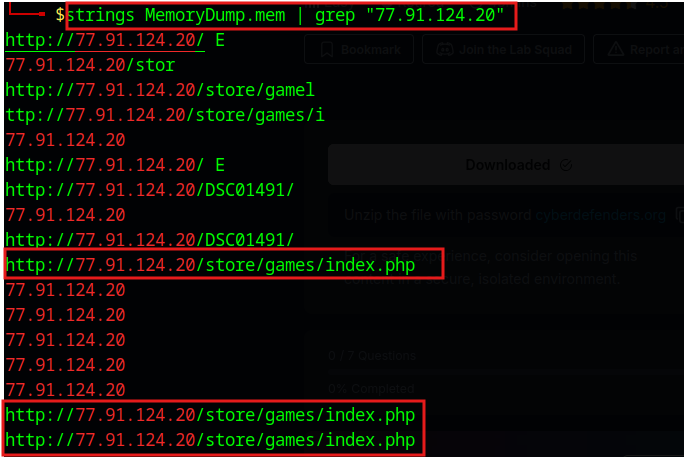


**Answer:** 77.91.124.20

**6. What is the full URL of the PHP file that the attacker visited?**

Since we know the IP address that the malicious program contacted, we can search fror strings in the memory dump which contains this IP address.

strings MemoryDump.mem | grep "77.91.124.20"

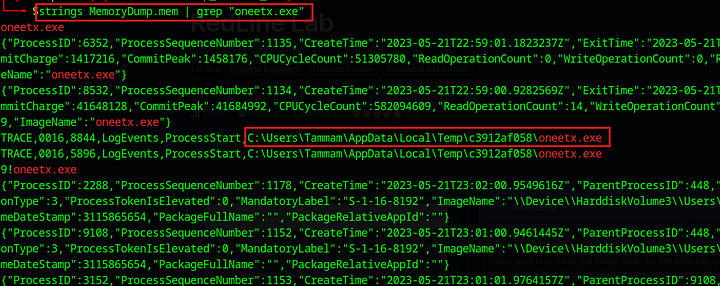


**Answer:** http://77.91.124.20/store/games/index.php

**7. What is the full path of the malicious executable?**

Search for the strings with oneetx.exe

strings MemoryDump.mem | grep "oneetx.exe"



**Answer:** C:\Users\Tammam\AppData\Local\Temp\c3912af058\oneetx.exe

This is the end of the walkthrough.