Mallox Evading AMSI

Published: 2023-12-27 · Archived: 2026-04-06 01:33:32 UTC

In the past, as blogged here, we have seen that the Mallox ransomware group has been targeting Indian companies since 2022. Recently, we noticed an update in their PowerShell script which is the crux of this blog. PowerShell scripts are an important part of the attack chain of Mallox attackers because after getting initial access to the machine using SQL or RDP, rest of the access like privilege escalation, executing Remcos RAT will be done using PowerShell only.

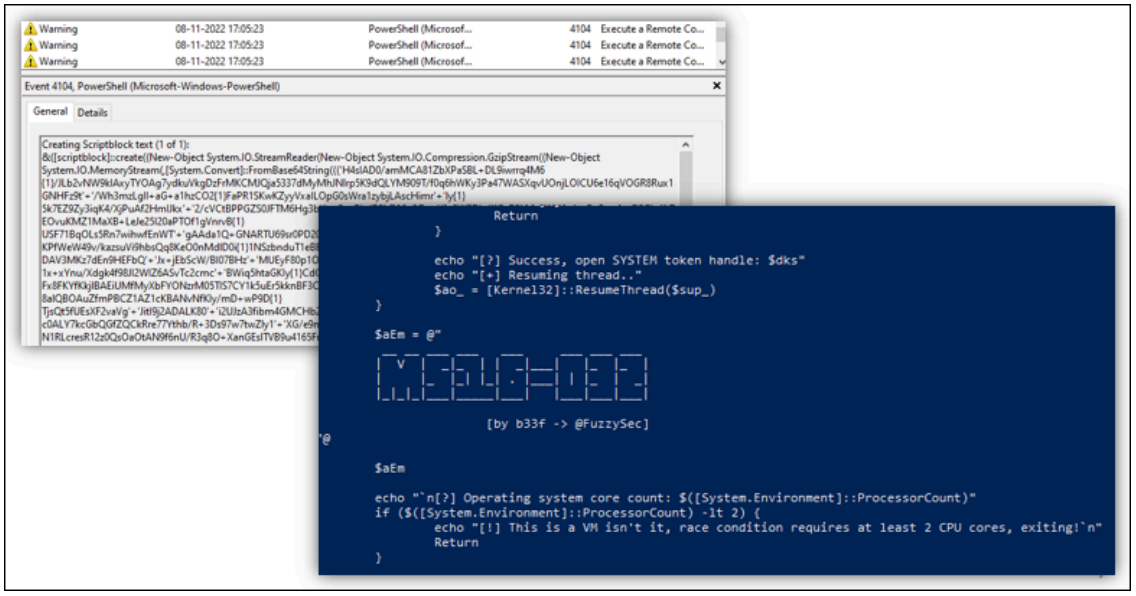

Figure 1: PowerShell script being used for MS16-032 privilege escalation

Figure 2: PowerShell script being used to download Mimikatz and run it

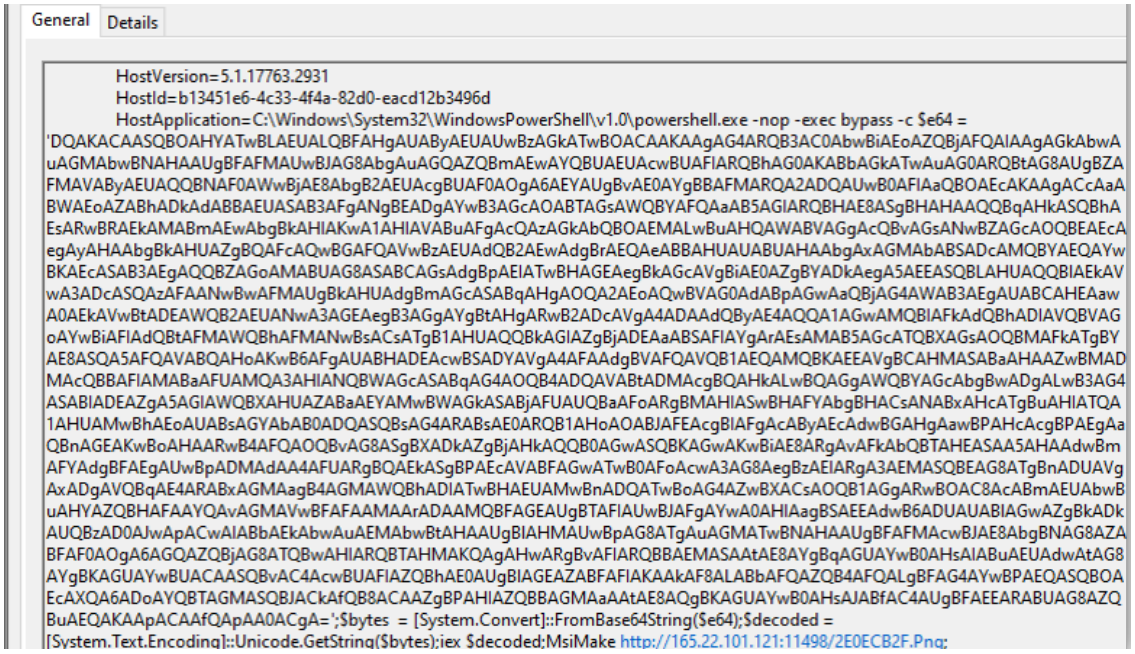

Figure 3: PowerShell being used for installing Remcos RAT

In their new updated powershell script, the attackers have included additional code which will attempt to bypass AV's AMSI detection component first; before running their regular code. AMSI (Anti Malware Scan Interface) is an interface in Windows OS which can be used by any application like an AV, to get the (mostly) deobuscated copy of the scripts like powershell, jscript and vbscript etc, before their execution. AVs can then scan these scripts and detect malicious scripts based on the AV's signature. To use this Interface, the applications have to register themselves by providing the dll path and the pointer to the function having scanning logic for the scripts.

The updated PowerShell script looks like this:

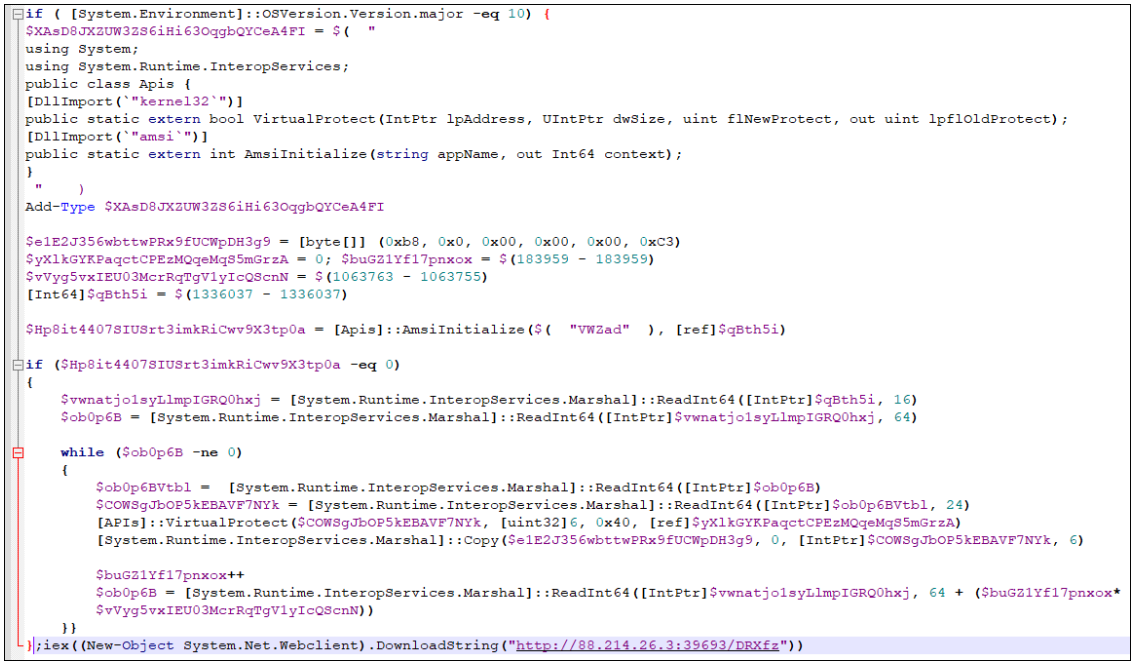

Figure 4: Latest PowerShell bypassing AMSI

This technique was developed and published by a Researcher named **Maor Korkos** in 2022. The mallox group has adopted the same and have started using it for bypassing.

The Script works as following :

1. The script imports Kernel32.dll and Amsi.dll and initialises VirtualProtect and AmsiInitialise APIs to be used later.

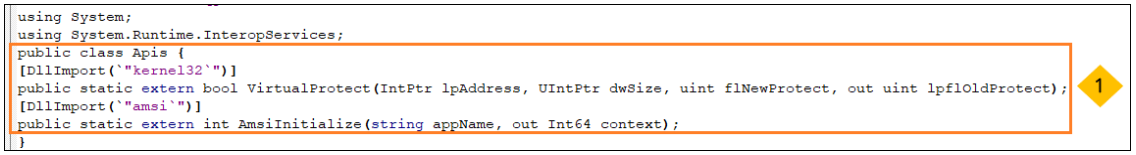

Figure 5: Importing Dll and Initializing APIs

2. A shellcode is kept stored in a variable to be copied into memory later. The purpose of this shellcode is to move 0x0 to EAX register and return.

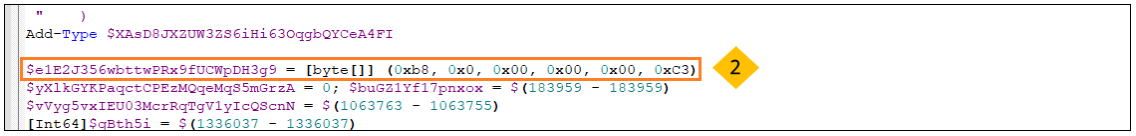

Figure 6: Shellcode

3. Then it calls AmsiInitialise API with the appname as **VWZad** which returns a pointer to amsicontext structure of type HAMSICONTEXT. This Structure mainly consist of following :
    - A signature, “AMSI” which defines the start of the structure.
    - Appname, which the application registered while initialising AMSI (**VWZad** in our case).
    - Mainly point to the address of the DLL and functions that AV vendors have registered with Windows to provide their anti malware capabilities to scan and detect malicious PowerShell scripts. The registered function will be invoked by the AmsiScanBuffer API whenever a PowerShell script is executed.
    - Session count.

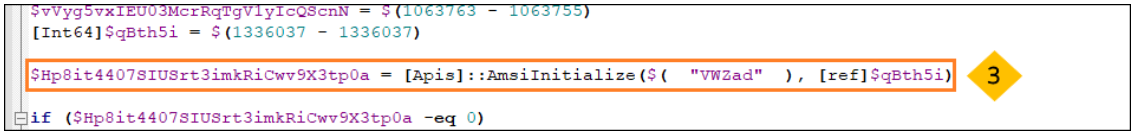

Figure 7: AmsiInitialise API being used

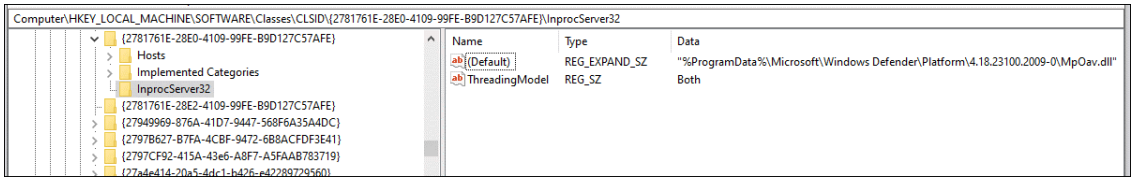

Figure 8: Windows defender registered dll for AMSI i.e MpOav.dll

4. After getting the pointer to amsicontext structure, the script traverses through the structure and finds the address of the function provided by the AV vendor. Then the script changes the permission of the .txt section of the MpOav.dll (Windows defender registered dll for AMSI) to

PAGE_EXECUTE_READWRITE so that it can copy the above-mentioned shellcode to the same function address to bypass it. As a result,the function's original content will be overwritten with the shellcode which will look like Figure 11. So now whenever the AMSI function runs for the current PowerShell session, it will return zero whenever a PowerShell script goes through AmsiScanBuffer, which will mean the AV have judged the PowerShell script as clean without even scanning it and will not be flagged

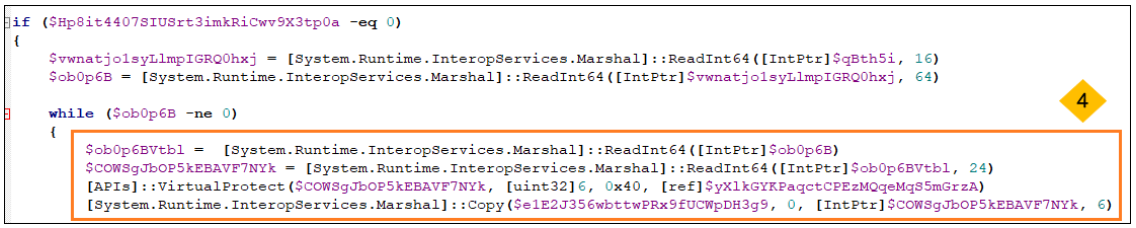

Figure 9: Patching shellcode in registered dll

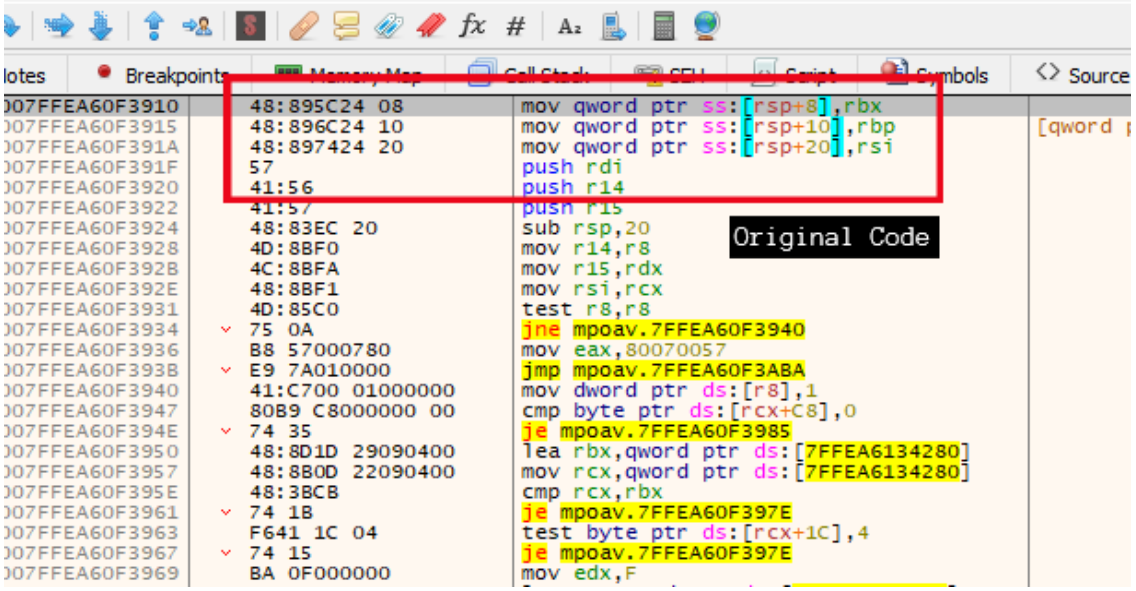

Figure 10: Mpoav.dll (Windows defender registered dll for AMSI) Original Code

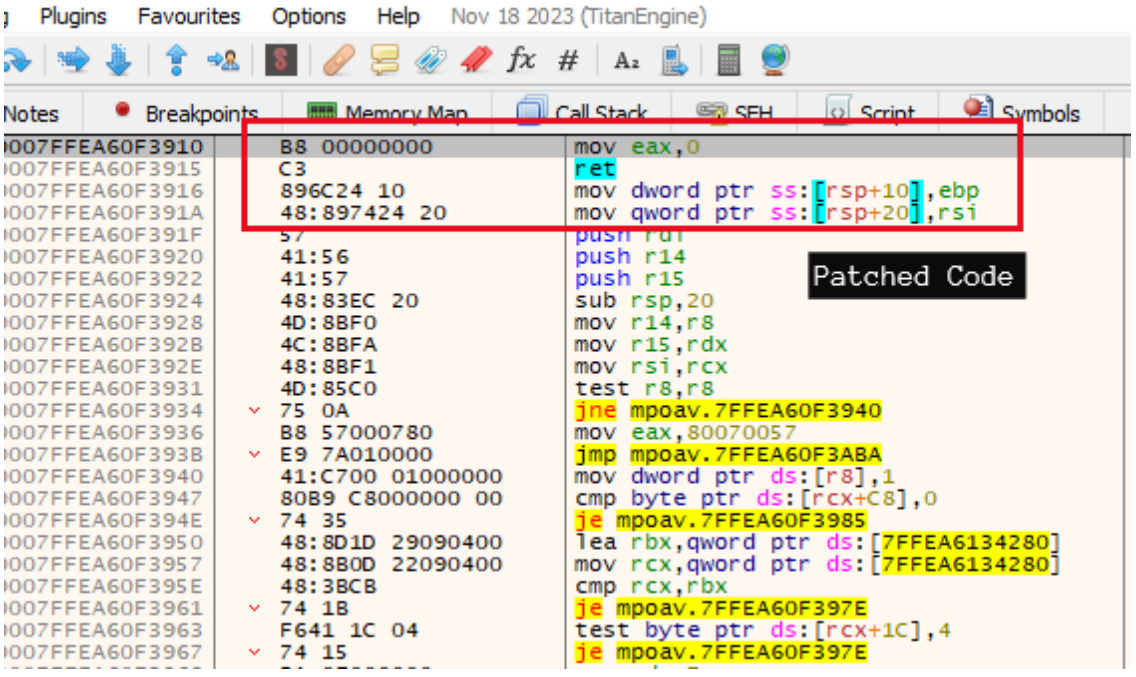

Figure 11: Mpoav.dll Patched Code

5. Now the script will move on to its main function which is to download the .NET downloader, without worrying if the AV is going to detect the script or not.

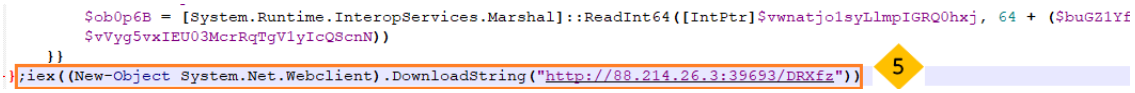

Figure 12: Final PS command to download malware

This is not the first time that Mallox group have improved their technique, they are doing this from time to time when AVs cause them issues by detecting their techniques. So we need to be a step ahead by keeping ourselves updated with the latest bypassing techniques used by threat actors. Protecting yourself by investing in a reputable security product such as K7 Antivirus is therefore necessary in today's world. We at K7 Labs provide detection for bypassing techniques like these and all the latest threats. Users are advised to use a reliable security product such as "K7 Total Security" and keep it up-to-date to safeguard their devices.

IOC

Hash
71BF701BE973F9477427E38FA39818BD

Source: https://labs.k7computing.com/index.php/mallox-evading-amsi/