July 18, 2020

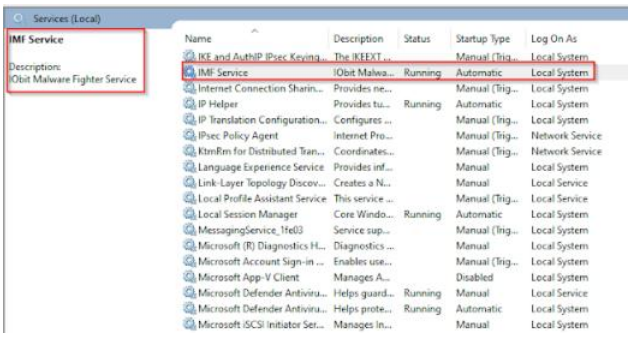
# IOBIT MALWARE FIGHTER - ARBITRARY CODE EXECUTION AS NT AUTHORITY\SYSTEM

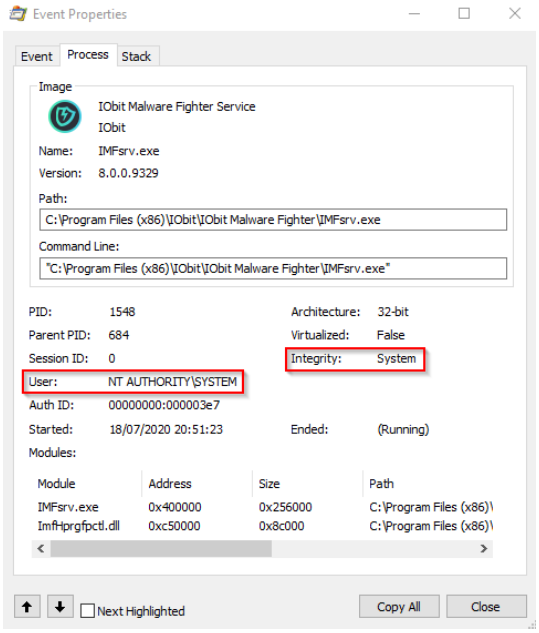
—

**Product:** IOBit Malware Fighter
**Version:** 8.0.2.547
**Tested on:** Windows 10 Pro 2004 x64
**Vendor informed:** No
**PoC:** This blog post
**CVE:** Requested


**Short Description:** A local attacker can use IOBit Malware Fighter to arbitrary execute code as NT Authority\System by placing a .dll file.

**Vulnerability Description:** IOBit Malware Fighter uses a service called "IMF Service" running as NT Authority\System.

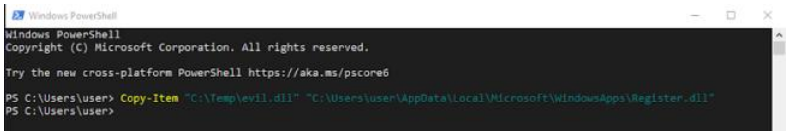




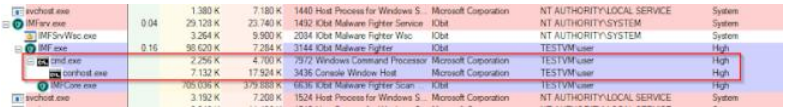

This service also spawn other Malware Fighter Processes (sub processes are "only" running elevated with high integrity).

To run code as NT Authority\System the attacker acts as following:

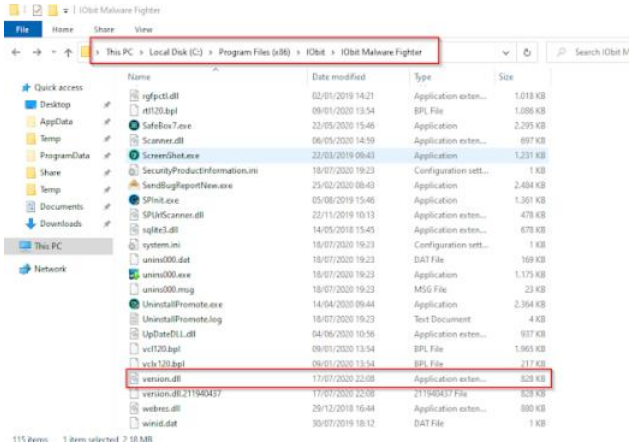
First the attacker drops a malicious dll file into "C:\Users\user\AppData\Local\Microsoft\WindowsApps" called "Register.dll".



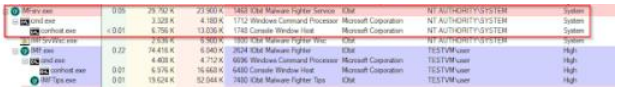

This file is executed when IOBit Malware Fighter is launched or the user opens Malware Fighter GUI with high integrity (admin rights).



Once the code runs with high integrity the same dll (evil.dll) will be copied to "C:\Program Files (x86)\IObit\IObit Malware Fighter" and called "version.dll"



With high integrity (admin rights) it is possible to reboot the system. Once the system is rebooted "version.dll" will be loaded by "IMFsrv.exe" as NT Authority\System:



**Conclusion:** I don´t know why IOBit Malware Fighter loads dll files from user locations or doesn´t validate files before loading or protects it´s installation folder...Classical dll hijacking and privilege escalation

Share

POPULAR POSTS

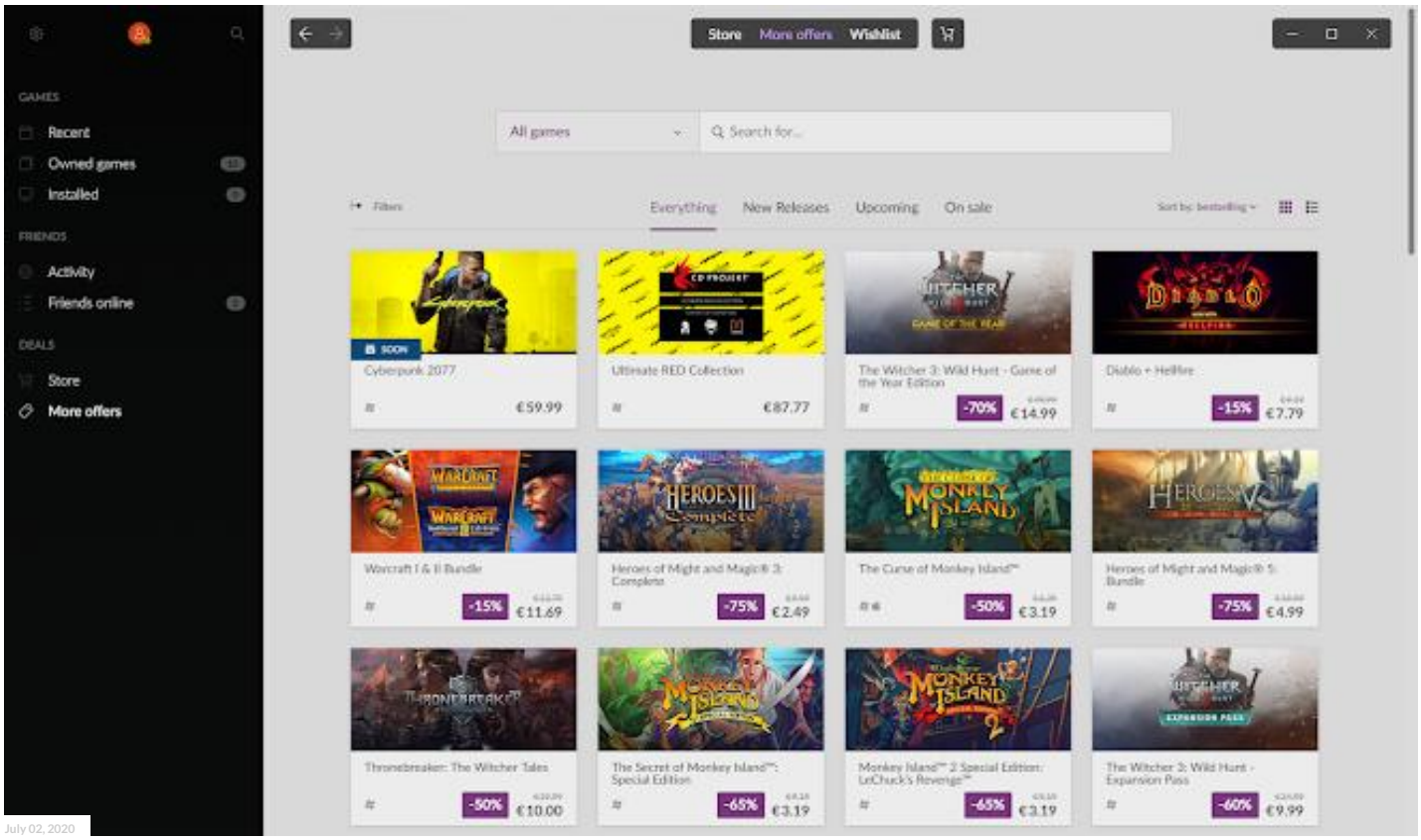
Showing 7 entries (filtered from **1,566** total entries) Search: winsat

| Auto-elevated ▲ | Executable | DLL | Procedure |
|---|---|---|---|
| ✔ | winsat.exe | d3d10_1.dll | DllMain |
| ✔ | | d3d10_1core.dll | DllMain |
| ✔ | | d3d10.dll | DllMain |
| ✔ | | d3d10core.dll | DllMain |
| ✔ | | d3d11.dll | DllMain |
| ✔ | | dxgi.dll | DllMain |
| ✔ | | winmm.dll | DllMain |

July 30, 2020

## UAC BYPASS VIA DLL HIJACKING AND MOCK DIRECTORIES

Share




July 02, 2020

GOG GALAXY - ESCALATION OF PRIVILEGES INCL. CODE EXECUTION

Share



Daniel Gebert

VISIT PROFILE

Archive

Report Abuse