

July 18, 2020

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

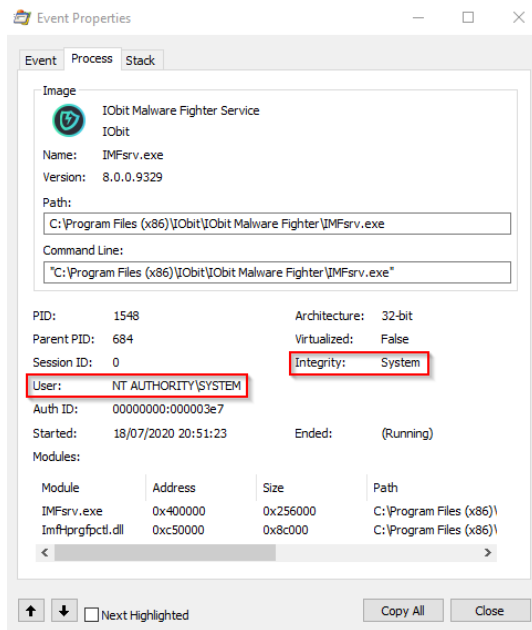
Product: IObit Malware Fighter  
Version: 8.0.2.547  
Tested on: Windows 10 Pro 2004 x64  
Vendor informed: No  
PoC: This blog post  
CVE: Requested



**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.

Services (Local)				
Name	Description	Status	Startup Type	Log On As
IMF Service	IObit Malwa...	Running	Automatic	Local System
Internet Connection Sharin...	Provides ne...	Running	Manual (Trig...	Local System
IP Helper	Provides ba...	Running	Automatic	Local System
IP Translation Configuration...	Configures ...	Running	Manual (Trig...	Local System
IPsec Policy Agent	Internet Pro...	Running	Manual (Trig...	Network Service
Kernel for Distributed Tran...	Coordinates...	Running	Manual (Trig...	Network Service
Language Experience Service	Provides inf...	Running	Manual	Local System
Link Layer Topology Discov...	Creates a NL...	Running	Manual	Local System
Local Profile Assistant Service	This service ...	Running	Manual (Trig...	Local System
Local Session Manager	Core Windo...	Running	Automatic	Local System
MessagingService, Heli...	Service sup...	Running	Manual (Trig...	Local System
Microsoft (R) Diagnostics H...	Diagnostics ...	Running	Manual	Local System
Microsoft Account Sign-in ...	Enables use...	Running	Manual (Trig...	Local System
Microsoft App-V Client	Manages A...	Running	Disabled	Local System
Microsoft Defender Antivir...	Helps guard...	Running	Manual	Local System
Microsoft Defender Antivir...	Helps prote...	Running	Automatic	Local System
Microsoft SCSI Initiator Ser...	Manages in...	Running	Manual	Local System

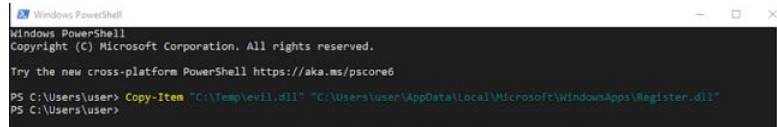


This service also spawn other Malware Fighter Processes (sub processes are "only" running elevated with high integrity).

svchost.exe	1.780 K	7.620 K	1460 Host Process for Windows S...	Microsoft Corporation	NT AUTHORITY\SYSTEM	System
IMFsrv.exe	0.13	29.384 K	23.632 K	1492 IObit Malware Fighter Service	IObit	NT AUTHORITY\SYSTEM
IMFsrvWsc.exe		2.628 K	6.880 K	2004 IObit Malware Fighter Wsc	IObit	NT AUTHORITY\SYSTEM
IMF.exe	0.27	74.000 K	12.540 K	4080 IObit Malware Fighter	IObit	TESTVM\User
IMFType.exe	0.02	19.952 K	51.860 K	7860 IObit Malware Fighter Type	IObit	TESTVM\User
IMFScan.exe		704.924 K	378.724 K	828 IObit Malware Fighter Scan	IObit	TESTVM\User
svchost.exe	< 0.01	1.132 K	7.192 K	1524 Host Process for Windows S...	Microsoft Corporation	NT AUTHORITY\LOCAL SERVICE
svchost.exe		2.456 K	11.532 K	1540 Host Process for Windows S...	Microsoft Corporation	NT AUTHORITY\LOCAL SERVICE

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

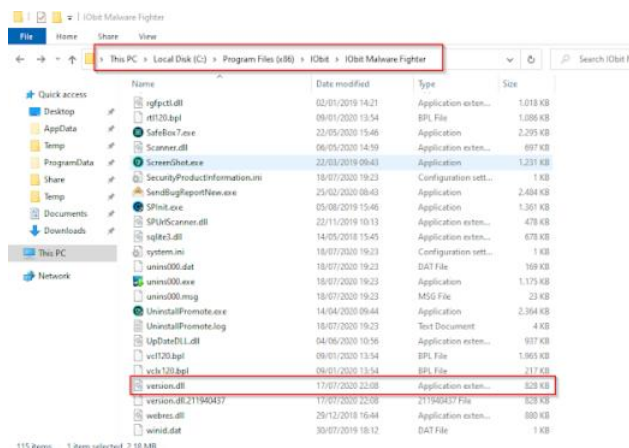
First the attacker drops a malicious dll file into "C:\Users\user\AppData\Local\Microsoft\WindowsApps" called "Register.dll".



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

svchost.exe	1.380 K	7.180 K	1480 Host Process for Windows S...	Microsoft Corporation	NT AUTHORITY\LOCAL SERVICE	System
IMFsrv.exe	0.04	29.128 K	23.740 K	1492 IObit Malware Fighter Service	IObit	NT AUTHORITY\SYSTEM
IMFsrvWsc.exe		3.264 K	9.900 K	2004 IObit Malware Fighter Wsc	IObit	NT AUTHORITY\SYSTEM
IMF.exe	0.15	98.020 K	7.284 K	3144 IObit Malware Fighter	IObit	TESTVM\User
IMFCore.exe		2.250 K	4.700 K	2972 Windows Command Processor	Microsoft Corporation	TESTVM\User
IMFCore.exe		7.132 K	17.924 K	3436 Console Window Host	Microsoft Corporation	TESTVM\User
IMFScan.exe		705.036 K	379.188 K	8636 IObit Malware Fighter Scan	IObit	TESTVM\User
svchost.exe		3.192 K	7.280 K	1524 Host Process for Windows S...	Microsoft Corporation	NT AUTHORITY\LOCAL SERVICE

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:

IOBit Malware Fighter.exe	0.00	28,702 K	21,900 K	1880 IObit Malware Fighter Service	Cmd	NT AUTHORITY\SYSTEM	System
cmd.exe	0.00	3,320 K	4,100 K	1712 Windows Command Processor	Microsoft Corporation	NT AUTHORITY\SYSTEM	System
cmd.exe	0.00	6,780 K	13,830 K	1780 Console Window Host	Microsoft Corporation	NT AUTHORITY\SYSTEM	System
IOBit Malware Fighter.exe	0.00	2,830 K	9,800 K	1880 IObit Malware Fighter Win	Cmd	NT AUTHORITY\SYSTEM	System
IOBit.exe	0.00	74,410 K	6,940 K	2824 IObit Malware Fighter	Cmd	TEST\VFuser	High
cmd.exe	0.00	4,400 K	4,720 K	6806 Windows Command Processor	Microsoft Corporation	TEST\VFuser	High
cmd.exe	0.00	6,370 K	16,460 K	6400 Console Window Host	Microsoft Corporation	TEST\VFuser	High
IOBit.exe	0.00	19,620 K	92,040 K	2880 IObit Malware Fighter Test	Cmd	TEST\VFuser	High

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)

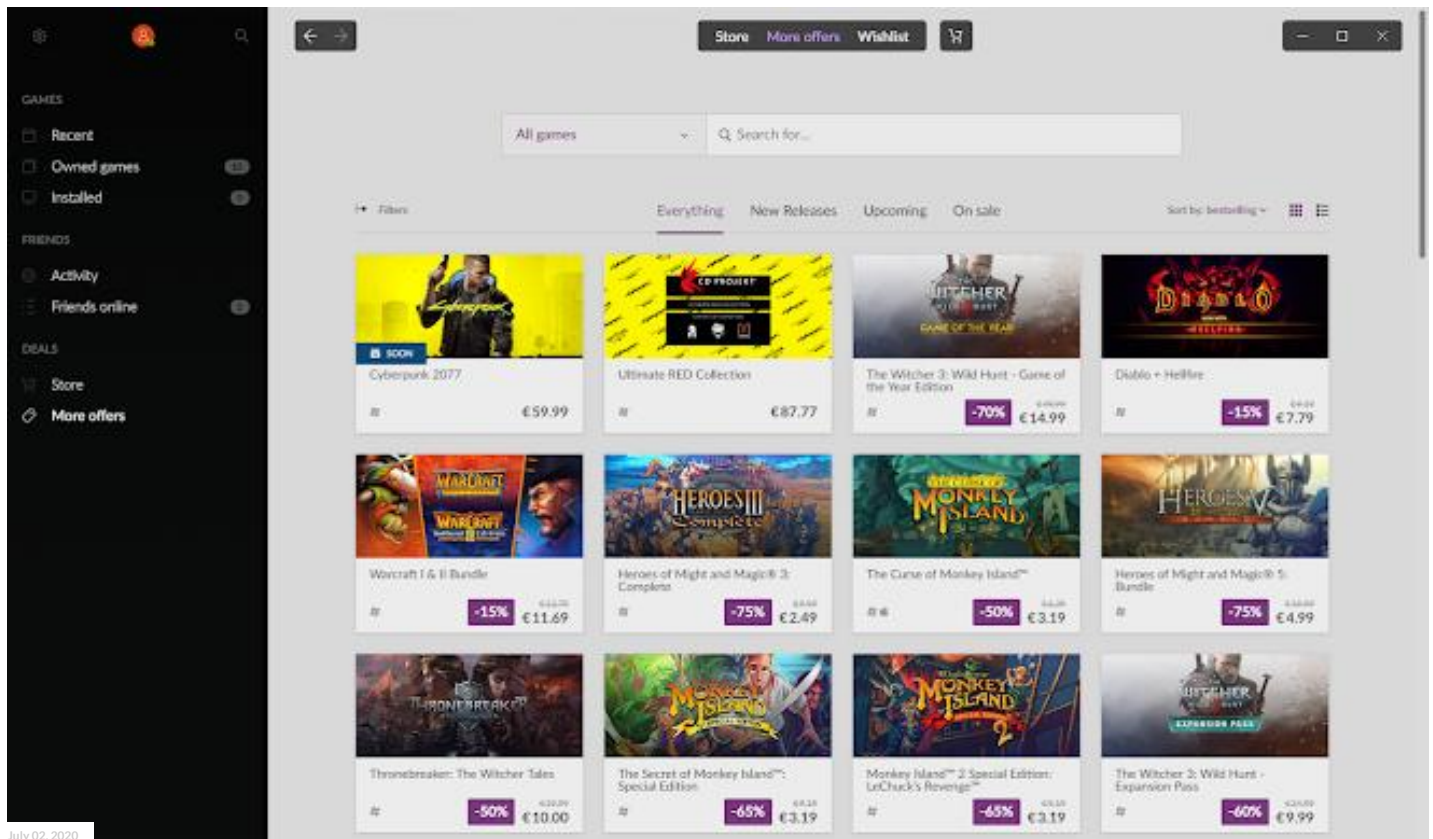
Search: winsat

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

Powered by Blogger

Theme images by enot-poloskun

Daniel Gebert

VISIT PROFILE

Archive

Report Abuse