ANOTHER IT SECURITY BLOG

IT Security, Hacking and More

June 29, 2020

WHEN YOUR ANTI VIRUS TURNS AGAINST YOU...

Product: IOBit Malware Fighter Pro
Version: 8.0.2.547
Tested on: Windows 10 Pro 2004 x64
Vendor informed: Yes
PoC: https://github.com/Daniel-itsec/Malwarefighter/blob/master/config.ini
CVE: 2020-15401

IObit Malware Fighter
v8.0.2.547

WARNING
This computer program is protected by copyright law and international treaties.

© IObit. All rights reserved.

[Bitdefender SDK]... © Bitdefender

All rights reserved.

EULA | Privacy Policy
Uninstall Instructions

Acknowledgements

Top Forum Contributors: enoskype, Scaman, Betahatme, Goku6354,Yuri B.M.
Top Beta Contributors: Adam Cullen, Ernie Andi McGeran, Filipe Pires, Leigh Eastwood, Louis Torrence, Michael Glasspool, Ray Haynes, Robert Meyer.
Arabic/العربية: Isalator zakom
Bulgarian/Български: Veli Lekov
Czech/Čeština: Jan Szotkowski
Danish/Dansk: Lars Andersen, Søren Mortensen
Dutch/Nederlands: Jil Nesten
Finnish/Suomi: Veikko Muurikainen
Flemish/Vlaams: Chris Verbeme
French/Français: Roland LALIS
German/Deutsch: Hans-Juergen Koppatz
Greek/Ελληνικά: Stathis Doukas
Hebrew/עברית: Eli Ben David
Hungarian/Magyar: Brechler Zsolt

After IOBit explained that they have a "great test team which fill all the bugs in our products" I thought it is a good idea to take a look at more products from IOBit and I found "IOBit Malware Fighter Pro". I spend only one evening in finding the bugs and playing around with Malware Fighter. I already thought that Malware Fighter Pro (or free) is full of bugs due to my last analysis of "IOBit Advanced System Care". The bugs I found can lead to a deactivation of **all** AV features incl. Windows Defender or simply just damage to the system. I created a real world scenario as a PoC.

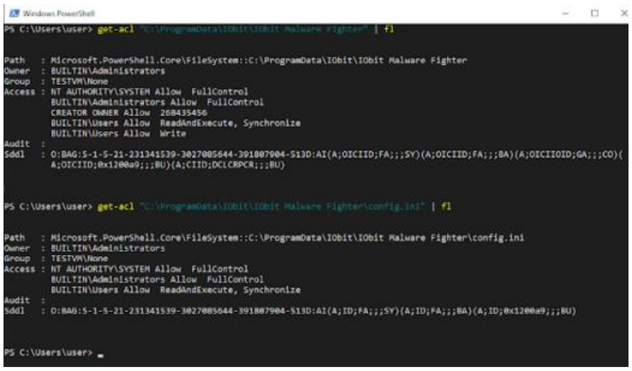
As every other AV solution also Malware Fighter (MF) uses a scan engine to detect malicious file and to remove/quarantine them after detection. Of course files/folders can also be added to a whitelist to exclude them from scanning and allow execution. In this example my goal is deactivate all Virus Scanner Features of Malware Fighter to allow eicar download and handling. Additionally I will lock MF for further usage and remove Microsoft Windows Defender to avoid having a AV solution on the system if MF is uninstalled.

MF runs under the highest possible level in Windows OS which is "NT AUTHORITY\SYSTEM". This is needed to remove malware which require higher access rights. When MF detects a malicious file it will

1. Automatically delete it/move to quarantine
2. Ask the user what to do with this file

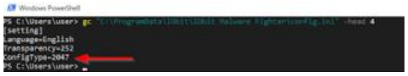
It doesn´t matter which method will be used it is still allowed for regular users to delete the file! This is possible because MF does set an delete oplock on the file and when set to "delete automatically" it will not delete the file when it is detected rather after over one second. I guess this is because MD does some additionally checks but I haven´t investigated this further. This brings an attacker into an interesting situation where the attacker can delete a file with SYSTEM rights. Also called arbitrary file deletion.

Malware Fighter uses the folder "C:\ProgramData\IObit\IObit Malware Fighter" to store configuration files. This folder is writable for regular users but they can not delete or write to existing files



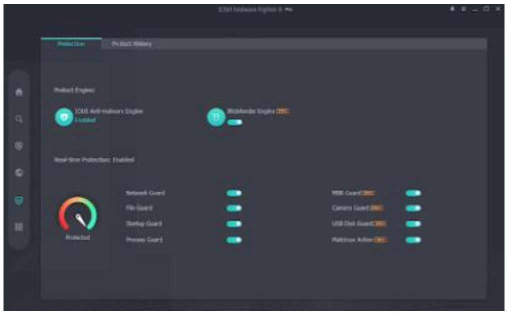
```
PS C:\Users\user> get-acl "C:\ProgramData\IObit\IObit Malware Fighter" | fl


Path   : Microsoft.PowerShell.Core\FileSystem::C:\ProgramData\IObit\IObit Malware Fighter
Owner  : BUILTIN\Administrators
Group  : TESTVM\None
Access : NT AUTHORITY\SYSTEM Allow  FullControl
         BUILTIN\Administrators Allow  FullControl
         CREATOR OWNER Allow  268435456
         BUILTIN\Users Allow  ReadAndExecute, Synchronize
         BUILTIN\Users Allow  Write
Audit  :
Sddl   : O:BAG:S-1-5-21-231341539-3027085644-391807904-513D:AI(A;OICIID;FA;;;SY)(A;OICIID;FA;;;BA)(A;OICIIOID;GA;;;CO)(
         A;OICIID;0x1200a9;;;BU)(A;CIID;DCLCRPCR;;;BU)



PS C:\Users\user> get-acl "C:\ProgramData\IObit\IObit Malware Fighter\config.ini" | fl


Path   : Microsoft.PowerShell.Core\FileSystem::C:\ProgramData\IObit\IObit Malware Fighter\config.ini
Owner  : BUILTIN\Administrators
Group  : TESTVM\None
Access : NT AUTHORITY\SYSTEM Allow  FullControl
         BUILTIN\Administrators Allow  FullControl
         BUILTIN\Users Allow  ReadAndExecute, Synchronize
Audit  :
Sddl   : O:BAG:S-1-5-21-231341539-3027085644-391807904-513D:AI(A;ID;FA;;;SY)(A;ID;FA;;;BA)(A;ID;0x1200a9;;;BU)


PS C:\Users\user> _
```

Malware Fighter uses the "C:\ProgramData\IObit\IObit Malware Fighter\config.ini" file to store its configuration. Some settings are presented just by a "1" others are presented by a numerical code. In config.ini the entry "ConfigType" holds the value which represents the actual configuration of MF.

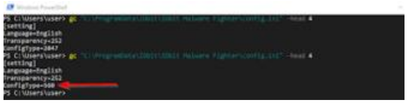


```
PS C:\Users\user> gc "C:\ProgramData\IObit\IObit Malware Fighter\config.ini" -head 4
[setting]
Language=English
Transparency=252
ConfigType=2047
PS C:\Users\user> _
```

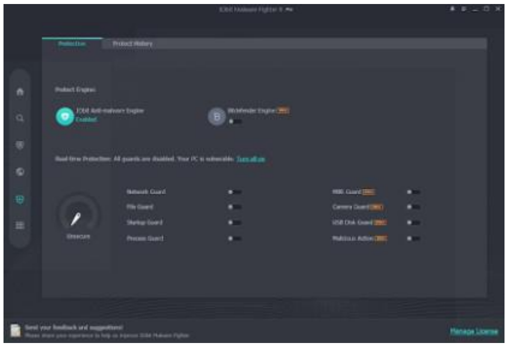
A value of "2047" means that all protection features are activated.



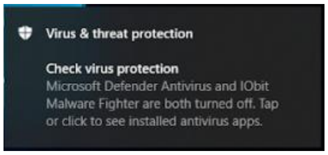
A value of "560" means settings are deactivated.



```
PS C:\Users\user> gc "C:\ProgramData\IObit\IObit Malware Fighter\config.ini" -head 4
[setting]
Language=English
Transparency=252
ConfigType=2047
PS C:\Users\user> gc "C:\ProgramData\IObit\IObit Malware Fighter\config.ini" -head 4
[setting]
Language=English
Transparency=252
ConfigType=560
PS C:\Users\user>
```


IObit Malware Fighter 8
Protection
Protect History
Protect Engines
IObit Anti-malware Engine
Enabled
Bitdefender Engine
Real-time Protection: All guards are disabled. Your PC is vulnerable. Turn all on
Network Guard
File Guard
Startup Guard
Process Guard
MBR Guard
Camera Guard
USB Disk Guard
Malicious Action
Unsecure
Send your feedback and suggestions!
Please share your experience to help us improve IObit Malware Fighter
Manage License

When all settings are deactivated users will also see this notification



Virus & threat protection

Check virus protection

Microsoft Defender Antivirus and IObit Malware Fighter are both turned off. Tap or click to see installed antivirus apps.

*A sample of a configuration file which turns off all settings can be found in the PoC link at the beginning of this article.

So how does the attack actual look like? Pretty easy:

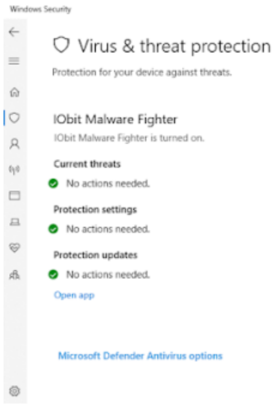
1. Create a malicious file (like eicar test file) *The file can be named keylogger.exe to scar users
2. Trigger the detection. This can be automatically or by just reading the file.
3. Remove the file
4. Create a NTFS folder junction and RPC link (pseudo-symlink). Good explanation about symlinks can be found here: https://offsec.almond.consulting/intro-to-file-operation-abuse-on-Windows.html
5. Wait until the file gets removed / moved to quarantine

Usually this is bad enough because it allows an attacker to delete system protected files like the hosts file. But we can extend this attack like this

1. Create a malicious file (like eicar test file)
2. Trigger the detection. This can be done automatically or by just reading the file
3. Remove the file
4. Create a NTFS folder junction and RPC link (pseudo-symlink) to Windows Defender executable ("C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.2006.8-0\MsMpEng.exe")
5. Wait until the file is removed. The filename will be saved and the selected operation (delete(move to quarantine) will be automatically executed without notifying the user
6. Repeat step 4 with "C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.2006.8-0\MsMpEng.exe" as target (version umber can be different)
7. Repeat step 4 with "C:\ProgramData\IObit\IObit Malware Fighter\config.ini" as target
8. Write a new config file. Malware Fighter will read the new settings shortly (few seconds)
9. *Additionally you can also replace the config files holding the whitelist entries ("C:\ProgramData\IObit\IObit Malware Fighter\sswlist.ini")

What will happen after following the above steps: Malware Fighter will first delete the Microsoft Windows Defender executables. After that MF will delete its own config file. And finally the new config file will be written. MF will shortly apply the settings stored in the (self written) config file.

It is also possible to delete "C:\Program Files (x86)\IObit\IObit Malware Fighter\IMF.exe". In this case MF Service will run as usual but it will do nothing. You can download the eicar file, run malware etc. the system is not protected. Due to the fact that MF main executable is missing it not possible to open MF anymore. Additionally Windows Defender will present this Window (because the Malware Fighter Service is still running)



Virus & threat protection

Protection for your device against threats.

IObit Malware Fighter

IObit Malware Fighter is turned on.

Current threats

No actions needed.

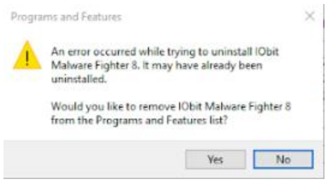
Protection settings

No actions needed.

Protection updates

No actions needed.

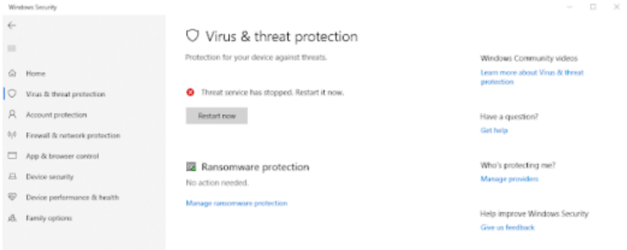
When also the uninstaller files are deleted the user will have a system with no working malware protection showing that the system is fully protected. When the user tries to uninstall this glorious software he or she will see this window



An error occurred while trying to uninstall IObit Malware Fighter 8. It may have already been uninstalled.

Would you like to remove IObit Malware Fighter 8 from the Programs and Features list?

If Microsoft Defender and IOBit Malware Fighter executables are deleted Windows Security will end up like this



Virus & threat protection

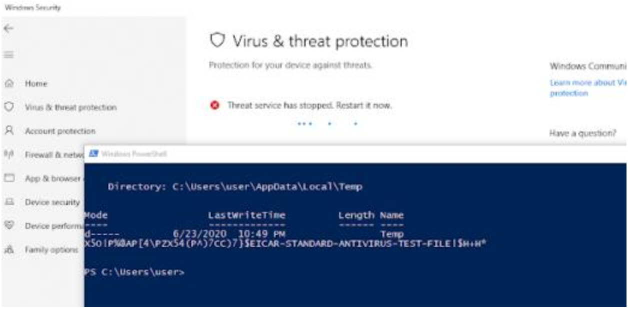
Protection for your device against threats.

Threat service has stopped. Restart it now.

Ransomware protection

No action needed.

Of course the service cannot be restarted because there is no executable to run and therefore there is no Virus protection



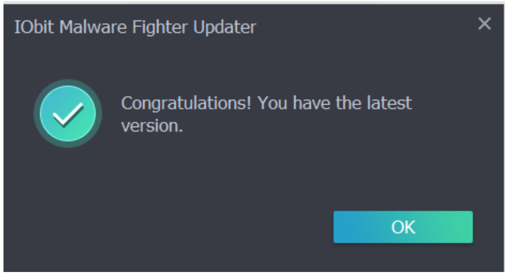
Virus & threat protection

Protection for your device against threats.

Threat service has stopped. Restart it now.

```
    Directory: C:\Users\user\AppData\Local\Temp

Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d-----        6/23/2020  10:49 PM                Temp
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*

PS C:\Users\user>
```

So I tried to run the Malware Fighter Updater; maybe this would repair the system?!? Instead I got congratulations from IOBit



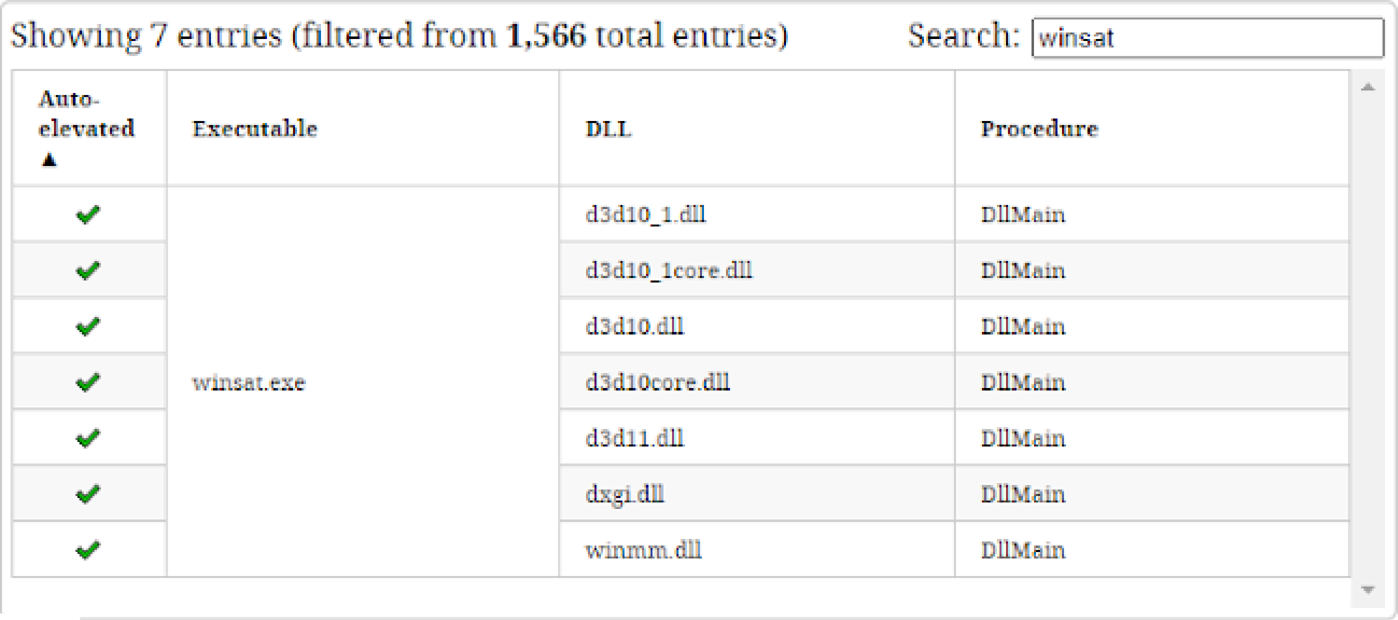
Congratulations! You have the latest version.

Personal note: Epic Fail

If Anti Virus software only needs a few lines of PowerShell to delete system files and **its own executables** this is really hard! It is easy to deactivate all features and leave the system vulnerable with Malware Fighter shwoing that everything is "Fully Protected". It is also easy to stay under the radar with a whitelist entry.

Share

POPULAR POSTS



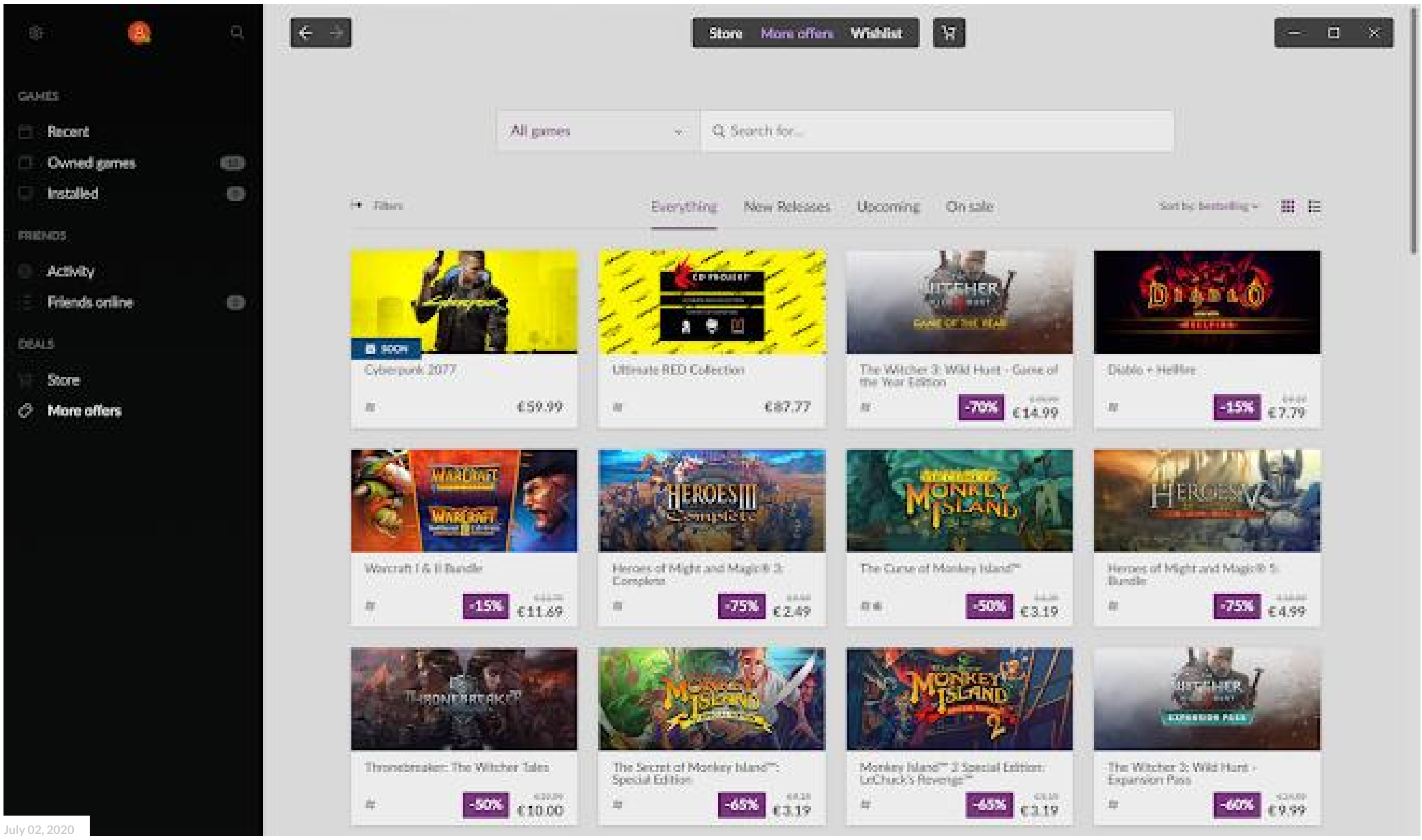
Showing 7 entries (filtered from 1,566 total entries) Search: winsat

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