ANOTHER IT SECURITY BLOG

IT Security, Hacking and More

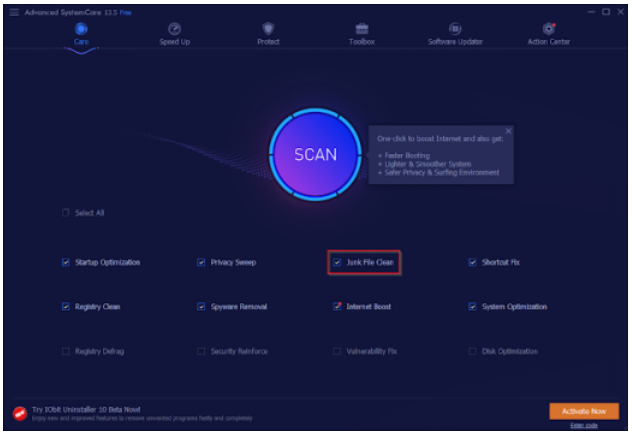
June 22, 2020

ARBITRARY FILE DELETION IN IOBIT ADVANCED SYSTEM CARE FREE 13.5.0.263 [CVE-2020-14990]

Product: IOBit Advanced System Care Free
Version: 13.5.0.263
Tested on: Windows 10 Pro 2004 x64
Vendor informed: Yes
PoC: https://github.com/Daniel-itsec/AdvancedSystemCare

Brief Description:
IOBit Advanced System Care Free and Pro (ASC) checks the OS for temporary files and deletes them to create free disk space. The scan and delete process are running in an elevated context (Administrator). ASC checks for files in \AppData\Local\Temp (%temp% environment variable) and mark files older then 24 hours for deletion. A malicious actor can wait for the ASC scan (wait for ASC.exe process) to start and write multiple files to %temp% and set the "LastWriteTime" timestamp on each file older than 24 hours. Shortly (about 1 second) after the file is created it will be deleted and replaced by a folder junction + RPC link (pseudo-symlink) by the attacker. Waiting 1 second will make sure that ASC detects the file as a temp file. When the user starts the clean operation or the clean operation is set to automatic ASC will follow the created pseudo-symlink and will delete the pseudo-symlink target (instead the original file) with elevated privileges (Administrator, integrity "high").

Vulnerability Explanation:
IOBit Advanced System Care (ASC) sets the "Junk File Clean" setting as default. So a user don´t have to select the feature manually.



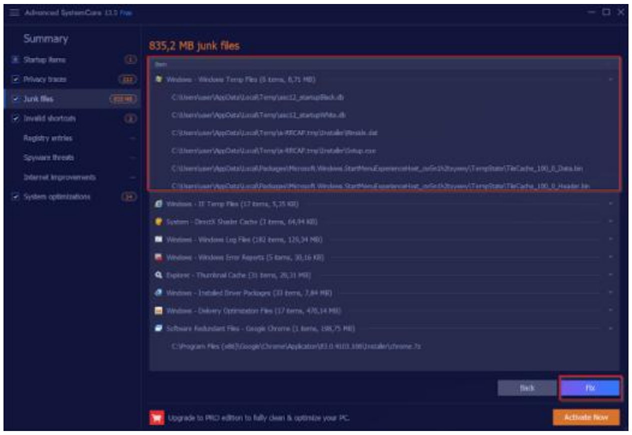
One-click to boost Internet and also get:
+ Faster Booting
+ Lighter & Smoother System
+ Safer Privacy & Surfing Environment

□ Select All

☑ Startup Optimization ☑ Privacy Sweep ☑ Junk File Clean ☑ Shortcut Fix
☑ Registry Clean ☑ Spyware Removal ☑ Internet Boost ☑ System Optimization
□ Registry Defrag □ Security Reinforce □ Vulnerability Fix □ Disk Optimization

Try IObit Uninstaller 10 Beta Now!
Enjoy new and improved features to remove unwanted programs fastly and completely

After the scan ASC shows the identified files. When the user clicks on "fix" the files will be deleted in an elevated context.

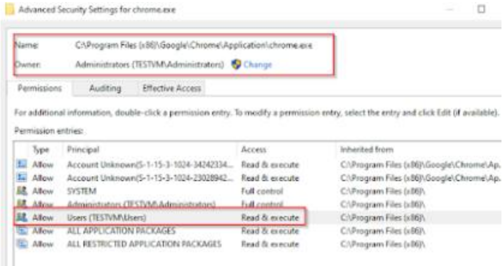


835,2 MB junk files

```
Windows - Windows Temp Files (8 items, 8,71 MB)
    C:\Users\user\AppData\Local\Temp\asc12_startupBlack.db
    C:\Users\user\AppData\Local\Temp\asc12_startupWhite.db
    C:\Users\user\AppData\Local\Temp\is-RRCAF.tmp\Installer\Resale.dat
    C:\Users\user\AppData\Local\Temp\is-RRCAF.tmp\Installer\Setup.exe
    C:\Users\user\AppData\Local\Packages\Microsoft.Windows.StartMenuExperienceHost_cw5n1h2txyewy\TempState\TileCache_100_0_Data.bin
    C:\Users\user\AppData\Local\Packages\Microsoft.Windows.StartMenuExperienceHost_cw5n1h2txyewy\TempState\TileCache_100_0_Header.bin
Windows - IE Temp Files (17 items, 5,35 KB)
System - DirectX Shader Cache (7 items, 64,94 KB)
Windows - Windows Log Files (182 items, 120,34 MB)
Windows - Windows Error Reports (5 items, 30,16 KB)
Explorer - Thumbnail Cache (31 items, 28,31 MB)
Windows - Installed Driver Packages (33 items, 7,84 MB)
Windows - Delivery Optimization Files (17 items, 476,14 MB)
Software Redundant Files - Google Chrome (1 items, 198,75 MB)
    C:\Program Files (x86)\Google\Chrome\Application\83.0.4103.106\Installer\chrome.7z
```

Upgrade to PRO edition to fully clean & optimize your PC.

Proof of Concept
In this example chrome.exe will be deleted. Chrome.exe can be accessed by regular users with read+execute rights; no right to delete nor full control.



Advanced Security Settings for chrome.exe

Name: C:\Program Files (x86)\Google\Chrome\Application\chrome.exe

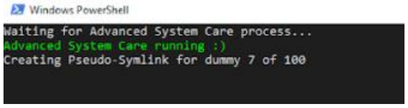
Owner: Administrators (TESTVM\Administrators) Change

For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).

Permission entries:

Type	Principal	Access	Inherited from
Allow	Account Unknown(S-1-15-3-1024-34242334...	Read & execute	C:\Program Files (x86)\Google\Chrome\Ap...
Allow	Account Unknown(S-1-15-3-1024-23028942...	Read & execute	C:\Program Files (x86)\Google\Chrome\Ap...
Allow	SYSTEM	Full control	C:\Program Files (x86)\
Allow	Administrators (TESTVM\Administrators)	Full control	C:\Program Files (x86)\
Allow	Users (TESTVM\Users)	Read & execute	C:\Program Files (x86)\
Allow	ALL APPLICATION PACKAGES	Read & execute	C:\Program Files (x86)\
Allow	ALL RESTRICTED APPLICATION PACKAGES	Read & execute	C:\Program Files (x86)\

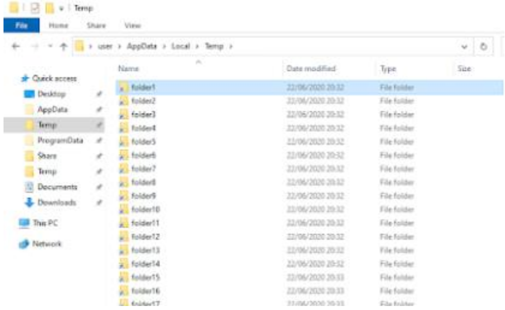
I wrote a script to automatize the attack. An attacker can wait for the ASC.exe process. Once the process is running the attacker will create dummy files in %temp% and replace them after one second with a pseudo-symlink to "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe". The scripts creates 100 pseudo-symlinks to make sure ASC will detect at least one file as a temp file.



Windows PowerShell

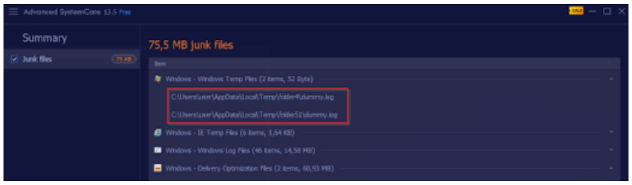
```
Waiting for Advanced System Care process...
Advanced System Care running :)
Creating Pseudo-Symlink for dummy 7 of 100
```

The temp folder it will look like this:



Name	Date modified	Type	Size
folder1	22/06/2020 20:32	File folder	
folder2	22/06/2020 20:32	File folder	
folder3	22/06/2020 20:32	File folder	
folder4	22/06/2020 20:32	File folder	
folder5	22/06/2020 20:32	File folder	
folder6	22/06/2020 20:32	File folder	
folder7	22/06/2020 20:32	File folder	
folder8	22/06/2020 20:32	File folder	
folder9	22/06/2020 20:32	File folder	
folder10	22/06/2020 20:32	File folder	
folder11	22/06/2020 20:32	File folder	
folder12	22/06/2020 20:32	File folder	
folder13	22/06/2020 20:32	File folder	
folder14	22/06/2020 20:32	File folder	
folder15	22/06/2020 20:33	File folder	
folder16	22/06/2020 20:33	File folder	
folder17	22/06/2020 20:33	File folder	

ASC will detect at least one file as a temp file and mark them for deletion



75,5 MB junk files

Windows - Windows Temp Files (2 items, 52 Byte)

C:\Users\user\AppData\Local\Temp\folder4\dummy.log

C:\Users\user\AppData\Local\Temp\folder51\dummy.log

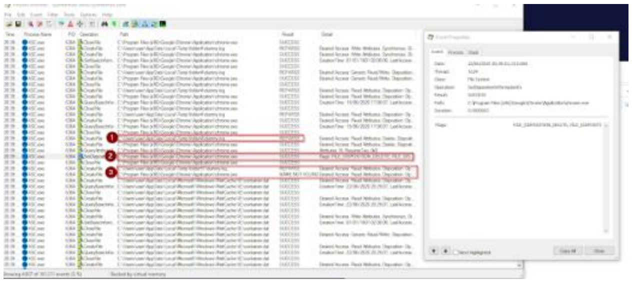
Windows - IE Temp Files (6 items, 1,64 KB)

Windows - Windows Log Files (46 items, 14,58 MB)

Windows - Delivery Optimization Files (2 items, 60,93 MB)

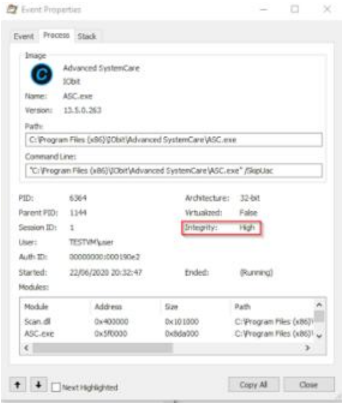
When things get "fixed"...

...the pseudo-symlink target will be deleted



1. ASC follows the reparse point
2. ASC deletes the file
3. A second dummy file was created but at this point the pseudo-symlink target was already deleted

This operation is performed with high integrity



Advanced SystemCare
IObit
Name: ASC.exe
Version: 13.5.0.263
Path:
C:\Program Files (x86)\IObit\Advanced SystemCare\ASC.exe
Command Line:
"C:\Program Files (x86)\IObit\Advanced SystemCare\ASC.exe" /SkipUac

PID: 6364
Parent PID: 1144
Session ID: 1
User: TESTVM\user
Auth ID: 00000000:000190e2
Started: 22/06/2020 20:32:47
Architecture: 32-bit
Virtualized: False
Integrity: High
Ended: (Running)
Modules:

Module	Address	Size	Path
Scan.dll	0x400000	0x101000	C:\Program Files (x86)\
ASC.exe	0x5f0000	0x8da000	C:\Program Files (x86)\

□ Next Highlighted

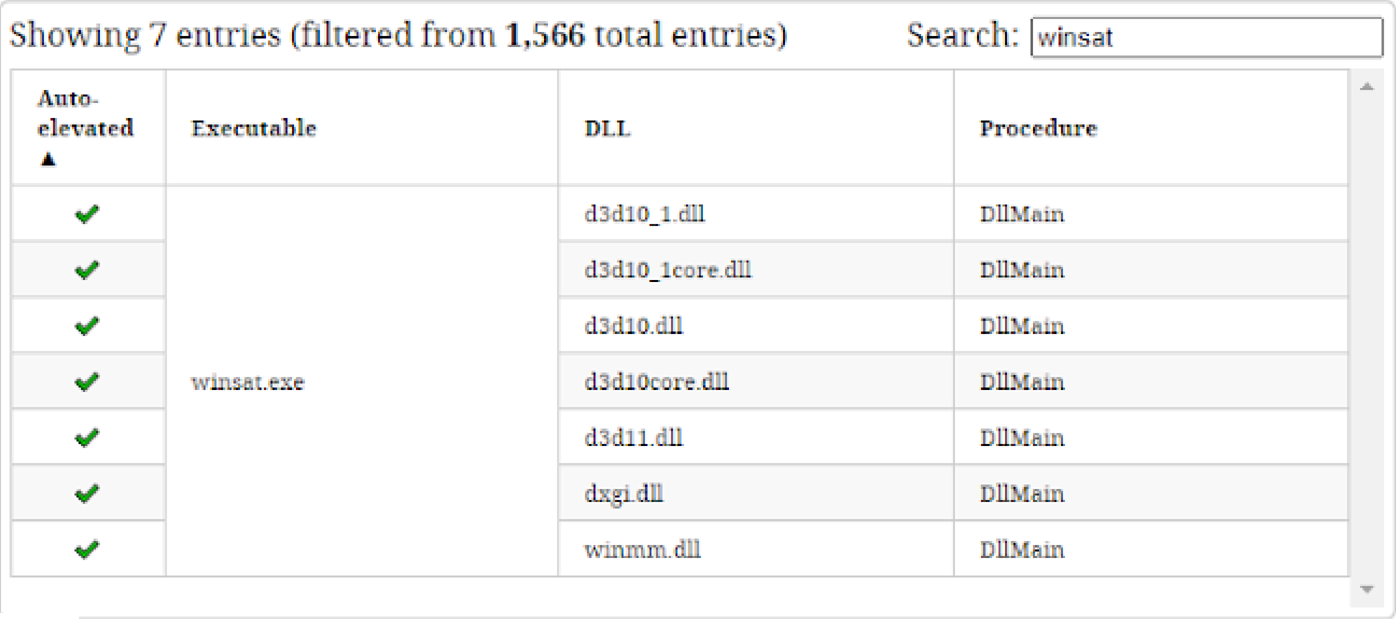
Conclusion: This attack can be avoided by checking reparse points and/or impersonating a user while performing delete operations in user controlled folders / on user controlled files.

Personal Note: I contacted IOBit to submit the bug. Unfortunately they were not interested because:

Presently we have a great test team which will find out all the bugs of our products.

Share

POPULAR POSTS



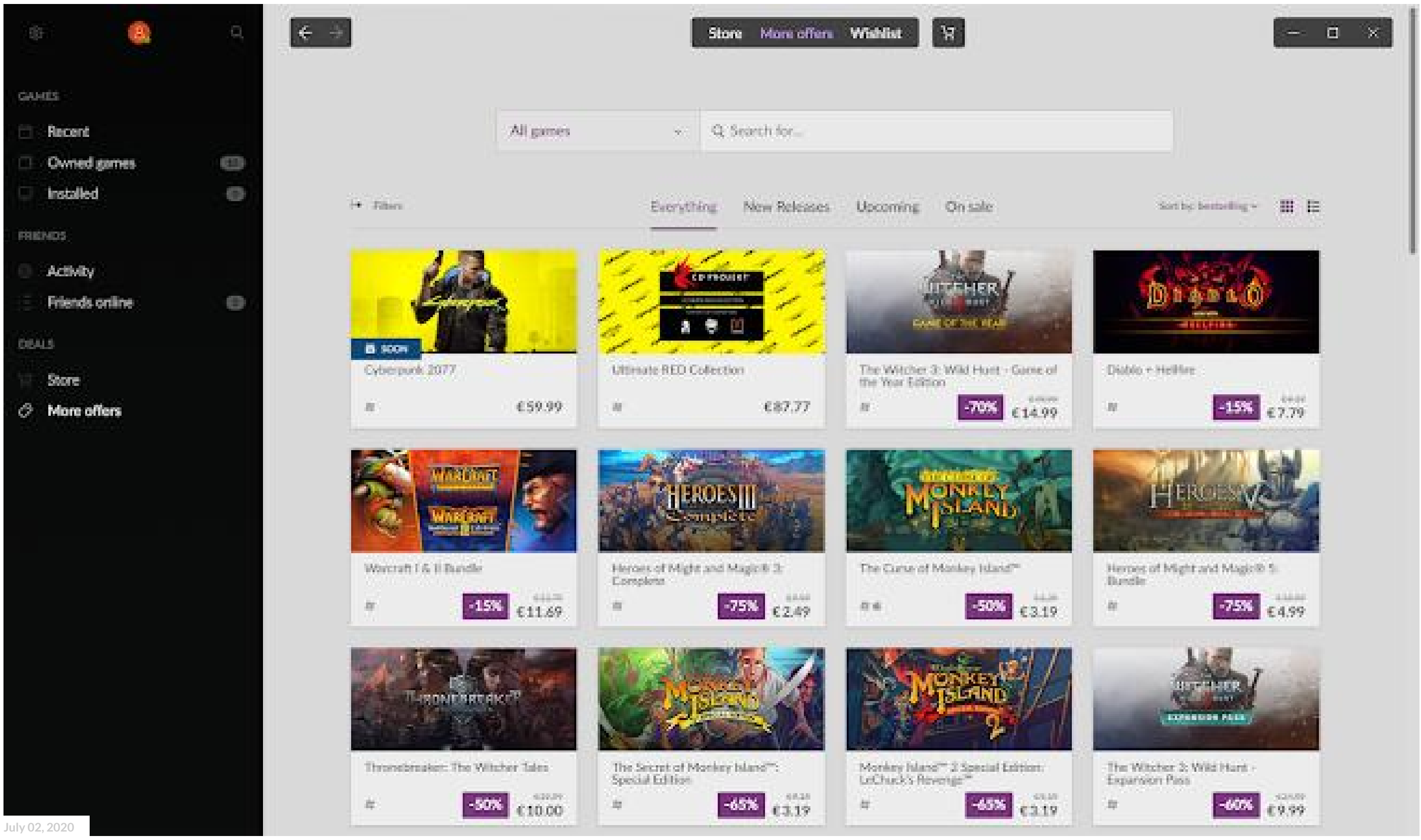
Showing 7 entries (filtered from **1,566** total entries) Search: winsat

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