Sysmon 14.0 — FileBlockExecutable

Olaf Hartong · Follow
3 min read · Aug 16, 2022

Sysmon now impedes executables, based on the file header from being written to the filesystem according to the filtering criteria. This can be a very powerful feature into blocking certain programs writing malicious files to disk. As a simple example, I've created this configuration that will not allow PE files from being written to the downloads directory.

Medium

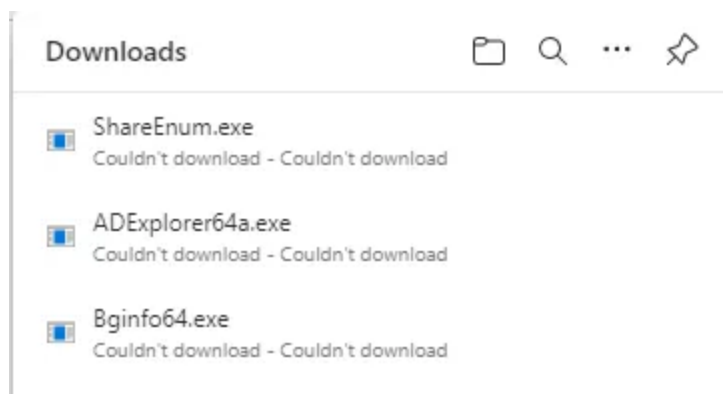Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

✦ Membership

✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app

When this configuration has been loaded and I attempt to download a file it will not work.
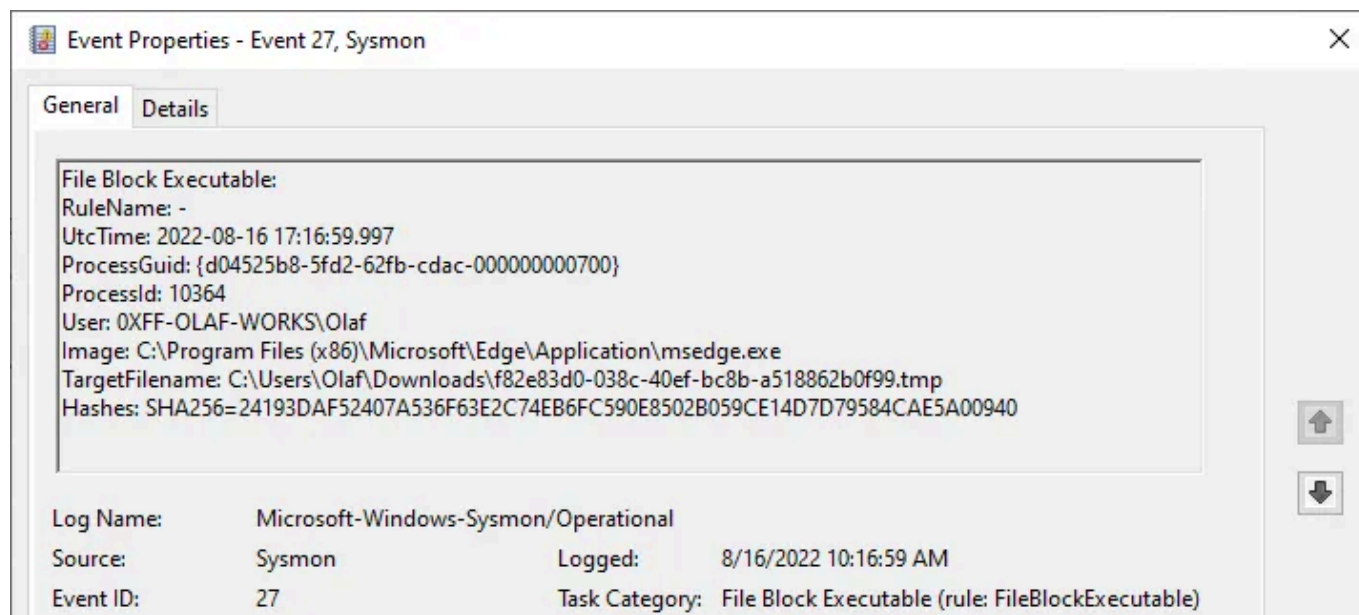

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Event Properties - Event 27, Sysmon ✕

General | Details

```
File Block Executable:
RuleName: -
UtcTime: 2022-08-16 17:16:59.997
ProcessGuid: {d04525b8-5fd2-62fb-cdac-000000000700}
ProcessId: 10364
User: 0XFF-OLAF-WORKS\Olaf
Image: C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
TargetFilename: C:\Users\Olaf\Downloads\f82e83d0-038c-40ef-bc8b-a518862b0f99.tmp
Hashes: SHA256=24193DAF52407A536F63E2C74EB6FC590E8502B059CE14D7D79584CAE5A00940
```

Log Name:	Microsoft-Windows-Sysmon/Operational		
Source:	Sysmon	Logged:	8/16/2022 10:16:59 AM
Event ID:	27	Task Category:	File Block Executable (rule: FileBlockExecutable)

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

✦ Membership

✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app

Powershell attempting to copy a file to the same folder.

While there is no error on the command line, the file is not written to disk. Sysmon prevented this, as the event below will show.

- the user who performed the action,

- which image/binary was used,

- the TargetFilename

- and the Hashes of the TargetFilename.

Sadly we do not have the OriginalFileName of the initiating Image (yet), which would make it even more robust in creating configurations as they are harder to change than the file name.

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

✦ Membership

✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app