

Medium

🔍


S

To make Medium work, we log user data. By using Medium, you agree to our [Privacy Policy](#), including cookie policy.


×

Sign up

Sign in




Sysmon 14.0 — FileBlockExecutable



Olaf Hartong · Follow

3 min read · Aug 16, 2022

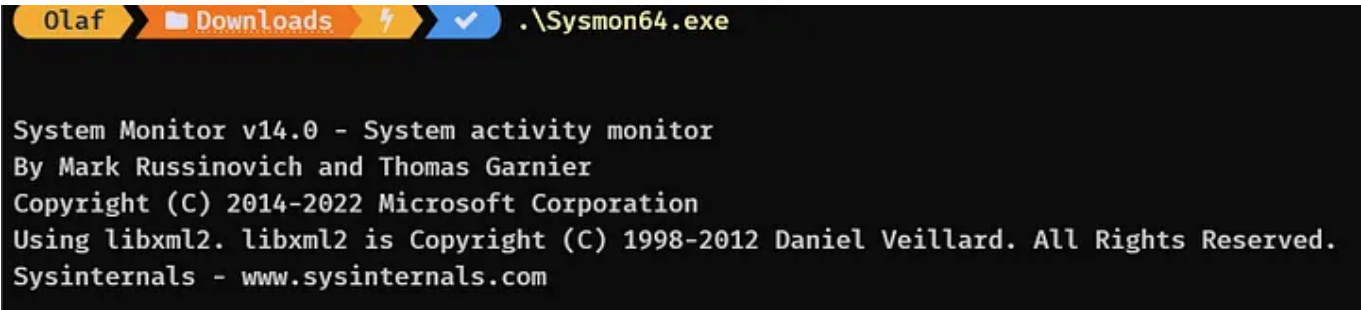
 210

 1









The Sysinternals team has released a new version of Sysmon. This brings the version number to 14.0 and raises the schema to 4.82.

Other than some fixes for several memory leaks that occurred in certain edge cases in the driver or between the driver and the service, there is a new event type! The new event has the ID of 27 and is called **FileBlockExecutable**.

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

×

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.

Sign up for free

★ Membership

✓

Read member-only stories

✓

Support writers you read most

✓

Earn money for your writing

✓

Listen to audio narrations

✓

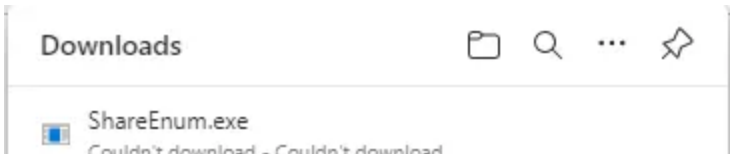
Read offline with the Medium app

Try for 5 \$/month

Page 1 of 7

To make Medium work, we log user data. By using Medium, you agree to our [Privacy Policy](#), including cookie policy.

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



Medium

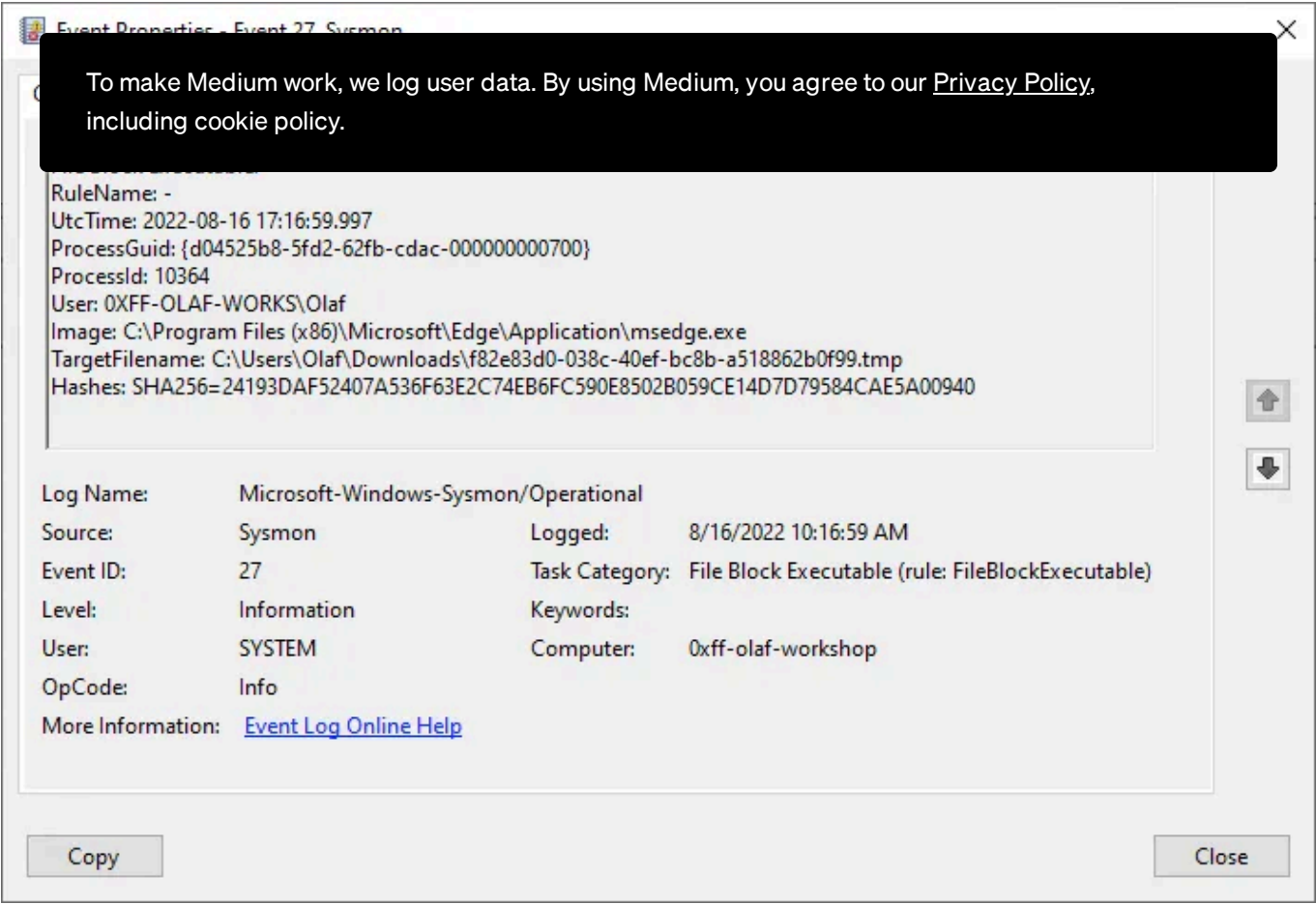
Sign up to discover human stories that deepen your understanding of the world.

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



Blocked file event ID 27 in the Event Log

The same is true for an DLL/XLL/WLL file since that will share the same MZ header.

Obviously doing this to the downloads folder is not something most people will use. Something more useful would for instance be writing executable files from Office processes, where a Macro might download a secondary payload and execute it.

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

Other considerations could be to prevent certain scripting tools, certain
ter
we

To make Medium work, we log user data. By using Medium, you agree to our [Privacy Policy](#),
including cookie policy.

cscrip.exe to not let it write files.

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.

PowerShell not being able to copy a file

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

of a workstation or function as an additional step in making it a bit more
ch

To make Medium work, we log user data. By using Medium, you agree to our [Privacy Policy](#), including cookie policy.

With all being said, this is an interesting move into not only logging but **also acting** here. I’m very keen to see what other features are considered for development by the SysInternals team. Obviously this requires a lot more testing, since you can impact operations significantly. And as always don’t test this in production, let it run for a while in a lab, then on a set of reference machines and then after some validation roll it out into prod.

Additionally, with new feature versions like this, there might be unkown issues. Rolling this into production is not recommended for a while.

- Sysmon
- Dfir
- Detection Engineering
- Infosec

 210

 1



Written by **Olaf Hartong**

2K Followers

Follow



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

To make Medium work, we log user data. By using Medium, you agree to our [Privacy Policy](#), including cookie policy.


 Olaf Hartong in FalconForce

Microsoft Defender for Endpoint Internals 0×02— Audit Settings...

In the previous article of this series, I’ve put Microsoft Defender for Endpoint (MDE) next...

Jul 1, 2022  87  1



 Olaf Hartong in FalconForce

Microsoft Defender for Endpoint Internals 0×04— Timeline

The MDE timeline has information which is not available in the advanced hunting...

Feb 10, 2023  82  4



See all from Olaf Hartong

Recommended from Medium

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


To make Medium work, we log user data. By using Medium, you agree to our [Privacy Policy](#), including cookie policy.

 Aardvark Infinity in Aardvark Infinity

Military-Grade Security Operations Center (SOC)

Setting up a Windows 11 system for a Military-Grade Security Operations Center (SOC)...

★ Oct 6 🖱️ 2 💬 1 

 Karthikeyan Nagaraj

Understanding Routing in Linux: Configuring Routes and Gateways

A Comprehensive Guide to Managing Routes and Gateways in Linux


★ Oct 20 🖱️ 972 💬 1 

 Sujit Mahakhud in InfoSec Write-ups

10 Common KQL Mistakes and How to Avoid Them

Non-members can read the blog through this link.

★ Sep 26 🖱️ 102 💬 2 

 Jashanpreet Singh

Day 2: Visualizing Your SOC Automation Lab 🤖

Welcome to Day 2 of the 10-Day SOC Innovation Series: Automation, Security, and...

★ Oct 16 🖱️ 7 💬 1 

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