User name:
Password:
Login / Forgot?
Register

Security Log | Windows | SharePoint | SQL Server | Exchange | | | Training | Tools | Newsletter | Webinars | Blog

Webinars | Training | Encyclopedia | Quick Reference | Book

Encyclopedia

- Event IDs
- All Event IDs
- Audit Policy

Go To Event ID: Go

Security Log Quick Reference Chart

Download now!

Sysmon Event ID 15

15: FileCreateStreamHash

Source	Sysmon

This is an event from Sysmon.

On this page

- Description of this event
- Field level details
- Examples

This event logs when a named file stream is created, and it generates events that log the hash of the contents of the file to which the stream is assigned (the unnamed stream), as well as the contents of the named stream. There are malware variants that drop their executables or configuration settings via browser downloads, and this event is aimed at capturing that based on the browser attaching a Zone.Identifier "mark of the web" stream.

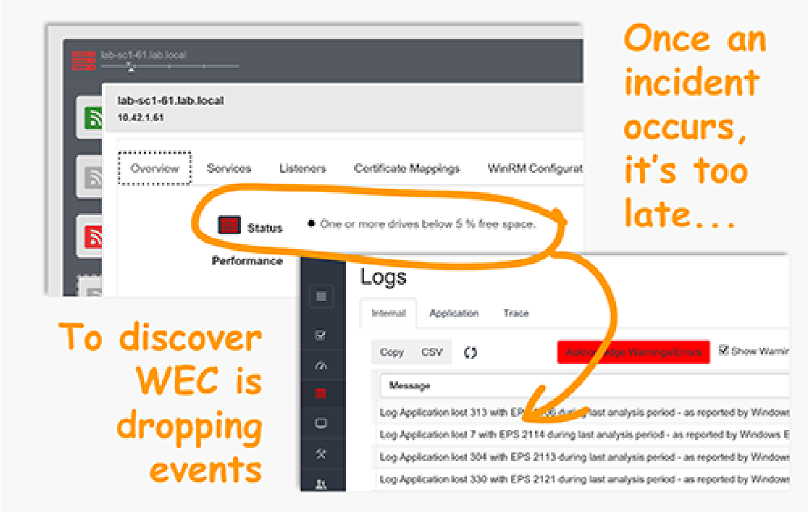
Free Security Log Resources by Randy

- Free Security Log Quick Reference Chart
- Windows Event Collection: Supercharger Free Edtion
- Free Active Directory Change Auditing Solution
- Free Course: Security Log Secrets

Description Fields in 15

- Log Name
- Source
- Date
- Event ID
- Task Category
- Level
- Keywords
- User
- Computer
- Description
- UtcTime
- ProcessGuid
- ProcessId
- Image
- TargetFileName
- CreationUtcTime
- Hash

Supercharger Enterprise



● One or more drives below 5 % free space.

```
Log Application lost 313 with EPS 2116 during last analysis period - as reported by Window
Log Application lost 7 with EPS 2114 during last analysis period - as reported by Windows E
Log Application lost 304 with EPS 2113 during last analysis period - as reported by Window
Log Application lost 330 with EPS 2121 during last analysis period - as reported by Window
```

Examples of 15

File stream created:
UtcTime: 2017-05-12 18:08:19.235
ProcessGuid: {a23eae89-c7f3-5915-0000-001083968417}
ProcessId: 26032
Image: C:\Program Files (x86)\WinMerge\WinMergeU.exe
TargetFilename: C:\repos\uws\Web\training\oiRegister.aspx.vb
CreationUtcTime: 2017-05-12 18:08:12.508

Hash: MD5=0825C513B61B70D0D47B110617DDD6E7,SHA256=29A25D16390F2A470D4742D41F447ED5FFCE58E93766B5A788BC
F36D94A2FCC

Top 10 Windows Security Events to Monitor

Free Tool for Windows Event Collection

Mini-Seminars Covering Event ID 15

- Using Sysmon v6.01 to Really See What's Happening on Endpoints; It's Better than the Windows Security Log
- Using New Events in Sysmon v13 to Detect Sophisticated Attacks

Upcoming Webinars

Additional Resources

Tweet Follow @randyfsmith

About | Newsletter | Contact

Disclaimer: We do our best to provide quality information and expert commentary but use all information at your own risk. For complaints, please contact abuse@ultimatewindowssecurity.com.

Terms of Use | Privacy |