

Sysmon'da Olayları HASH Değerlerine Göre İnceleme ve Yorumlama

Olay kayıtları alındığında bir çok işleme ait hash bilgiside alınır. Bir işlemin şüpheli olup olmadığı bu hashler yardımıyla anlaşılabilir. Herhangi bir olaya tıklandığında hash bilgisi virustotal tarzı hizmetler yardımıyla şüpheli olup olmadığı anlaşılabilir.

The screenshot shows the Sysmon Event Viewer interface. On the left, there is a tree view of event categories. The main pane displays a list of events with columns for Level, Date and Time, Source, and Event ID. A specific event is selected, and its details are shown in the right pane. The details include the event name, source, and a list of attributes. The 'Hashes' attribute is highlighted, showing the SHA-256 hash of the file.

Düzye	Tarih ve Saat	Kaynak	Olay Kimliği	Göre
Bilgi	3.10.2023 14:16:25	Sysmon	1	Proce
Bilgi	3.10.2023 14:16:10	Sysmon	5	Proce
Bilgi	3.10.2023 14:16:06	Sysmon	5	Proce
Bilgi	3.10.2023 14:16:06	Sysmon	1	Proce
Bilgi	3.10.2023 14:16:05	Sysmon	1	Proce
Bilgi	3.10.2023 14:16:05	Sysmon	5	Proce
Bilgi	3.10.2023 14:16:05	Sysmon	5	Proce

Olay 1, Sysmon

Genel Açıklamalar

Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: svchost.exe
CommandLine: C:\Windows\System32\svchost.exe -k netsvc -p -s NetSetupSvc
CurrentDirectory: C:\Windows\system32
User: NT AUTHORITY\SYSTEM
LogonId: {6f59d4e4-9862-651a-e703-000000000000}
LogonId: 0x3e7
TerminalSessionId: 0
IntegrityLevel: System
Hashes: SHA-256: A0D683A6910A8B8BF0E28B557FAD00BA98166794932AF2ACA069D9AA19EABFE88
ParentProcessId: {6f59d4e4-9862-651a-e703-000000000000}
ParentProcessId: 620
ParentImage: C:\Windows\System32\services.exe
ParentCommandLine: C:\Windows\System32\services.exe
ParentUser: NT AUTHORITY\SYSTEM

Günlük Adı: Microsoft-Windows-Sysmon/Operational
Kaynak: Sysmon
Günlük kaydedilen: 3.10.2023 14:16:06
Olay Kimliği: 1
Görev Kategorisi: Process Create (rule: ProcessCreate)
Düzye: Bilgi
Anahtar Sözcükler:
Kullanıcı: SYSTEM
Bilgisayar: DESKTOP-SVAKPLUJ
İşlem kodu: Bilgi
Ek Bilgi: [Olay Günlüğü Çevrimiçi Yardımı](#)

The screenshot shows the VirusTotal analysis results for the file svchost.exe. The file is identified as 'File distributed by Microsoft'. The analysis shows that the file is safe, with a score of 0/172. The file is 54.02 KB in size and was last analyzed 16 minutes ago. The analysis was performed by the EXE engine.

0 / 172

File distributed by Microsoft

add683a6910abbf0e28b557fad00ba98166794932ae2aca069d9aa19ea8fe88

svchost.exe

Size: 54.02 KB
Last Analysis Date: 16 minutes ago

peexe assembly overlay signed detect-debug-environment idle 64bits known-distributor

Community Score

Virustotal ile incelenen bu olayın normal bir durum olduğu bu şekilde anlaşılabilir.

Revision #2

Created 27 January 2024 16:04:19 by Ertan Sözer

Updated 27 January 2024 16:05:17 by Ertan Sözer