sdelete

- Table of Contents

Open all sections | Close all sections

- Tool Overview

Category

Deleting Evidence

Description

Deletes a file after overwriting it several times.

Example of Presumed Tool Use During an Attack

This tool is used to delete a file created in the course of an attack to make recovery impossible.

- Tool Operation Overview

Item	Description
OS	Windows
Belonging to Domain	Not required
Rights	Standard user

- Information Acquired from Log

Standard Settings

- Host
  - A registry value created when the sdelete License Agreement has been agreed to (registry).
  - Execution history (Prefetch)

Additional Settings

- Host
  - Execution history (audit policy, Sysmon)
  - A record of deleting and overwriting the file during the audit of object access (audit policy).

- Evidence That Can Be Confirmed When Execution is Successful

- In the Event ID: 4656 of the event log "Security", files with distinctive file names have been deleted. Name of a file deleted by sdelete is partially replaced with other letters. (In the case of "sdelete.txt", the file name may be changed to "sdeleAAAAAAAAAAAAAAAAAAAA.AAA", for example.)

- Main Information Recorded at Execution

- Host

USN journal

#	File Name	Process
1	[File to be Deleted]	CLOSE+FILE_DELETE
2	[Executable File Name of Tool]-[RANDOM].pf	FILE_CREATE
3	[Executable File Name of Tool]-[RANDOM].pf	DATA_EXTEND+FILE_CREATE
4	[Executable File Name of Tool]-[RANDOM].pf	CLOSE+DATA_EXTEND+FILE_CREATE

Event log

#	Log	Event ID	Task Category	Event Details
1	Microsoft-Windows-Sysmon/Operational	1	Process Create (rule: ProcessCreate)	Process Create. • **CommandLine**: Command line of the execution command • **UtcTime**: Process execution date and time (UTC) • **ProcessGuid/ProcessId**: Process ID • **Image**: Path to the executable file (path to the tool) • **User**: Execute as user
2	Security	4656	File System/Other Object Access Events	A handle to an object was requested. • **Access Request Information > Access/Reason for Access/Access Mask**: Requested privilege (DELETE) • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of the user who executed the tool • **Process Information > Process Name**: Name of the process that closed the handle (path to the tool) • **Object > Object Name**: Target file name (file to be deleted)
3	Security	4656	File System/Other Object Access Events	A handle to an object was requested. • **Access Request Information > Access/Reason for Access/Access Mask**: Requested privileges (WriteData or AddFile, AppendData) • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of the user who executed the tool • **Object > Object Name**: Target file name (file to be deleted)

UserAssist

#	Registry	Data
1	\REGISTRY\USER\[User SID]\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{[GUID]}\Count\[ROT13 of Path]\[ROT13 of Executable File Name]	Date and time of the initial execution, Total number of executions

MFT

#	Path	Header Flag	Validity
1	[Drive Name]:\Windows\Prefetch\[Executable File Name of Tool]-[RANDOM].pf	FILE	ALLOCATED
2	[File to be Deleted]	-	(to be deleted)

Prefetch

- C:\Windows\Prefetch\[Executable File Name of Tool]-[RANDOM].pf

Registry entry

#	Path	Value
1	HKEY_USERS\[User SID]\SOFTWARE\Sysinternals\Sdelete	0x00000001

- Details: Host

- USN Journal

#	File Name	Process	Attribute
1	[File to be Deleted]	CLOSE+FILE_DELETE	archive
2	[Executable File Name of Tool]-[RANDOM].pf	FILE_CREATE	archive+not_indexed
	[Executable File Name of Tool]-[RANDOM].pf	DATA_EXTEND+FILE_CREATE	archive+not_indexed
	[Executable File Name of Tool]-[RANDOM].pf	CLOSE+DATA_EXTEND+FILE_CREATE	archive+not_indexed

- Event Log

#	Event Log	Event ID	Task Category	Event Details
1	Microsoft-Windows-Sysmon/Operational	1	Process Create (rule: ProcessCreate)	Process Create. • **LogonGuid/LogonId**: ID of the logon session • **ParentProcessGuid/ParentProcessId**: Process ID of the parent process • **ParentImage**: Executable file of the parent process • **CommandLine**: Command line of the execution command • **ParentCommandLine**: Command line of the parent process • **UtcTime**: Process execution date and time (UTC) • **ProcessGuid/ProcessId**: Process ID • **User**: Execute as user • **Hashes**: Hash value of the executable file • **Image**: Path to the executable file (path to the tool)
	Security	4688	Process Create	A new process has been created. • **Process Information > Required Label**: Necessity of privilege escalation (Mandatory Label\Medium Mandatory Level) • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of the user who executed the tool • **Process Information > Source Process Name**: Path to the parent process that created the new process. A record is confirmed on Windows 10 only. • **Log Date and Time**: Process execution date and time (local time) • **Process Information > New Process Name**: Path to the executable file (path to the tool) • **Process Information > Token Escalation Type**: Presence of privilege escalation (1) • **Process Information > New Process ID**: Process ID (hexadecimal) • **Process Information > Source Process ID**: Process ID of the parent process that created the new process. "Creator Process ID" in Windows 7 • **Subject > Logon ID**: Session ID of the user who executed the process
2	Microsoft-Windows-Sysmon/Operational	12	Registry object added or deleted (rule: RegistryEvent)	Registry object added or deleted. • **EventType**: Process type (CreateKey) • **Image**: Path to the executable file (C:\Windows\System32\svchost.exe) • **TargetObject**: Created/deleted registry key/value (\REGISTRY\A\[GUID]\Root\File\[GUID])
	Microsoft-Windows-Sysmon/Operational	12	Registry object added or deleted (rule: RegistryEvent)	Registry object added or deleted. • **EventType**: Process type (CreateKey) • **Image**: Path to the executable file (C:\Windows\System32\svchost.exe) • **TargetObject**: Created/deleted registry key/value (\REGISTRY\A\[GUID]\Root\File\[GUID]\30000191d0)

	Microsoft-Windows-Sysmon/Operational	13	Registry value set (rule: RegistryEvent)	Registry value set. • **EventType**: Process type (SetValue) • **Image**: Path to the executable file (C:\Windows\System32\svchost.exe) • **Details**: Setting value written to the registry (path to the tool) • **TargetObject**: Registry value at the write destination (\REGISTRY\A\[GUID]\Root\File\[GUID]\30000191d0\15)
	Microsoft-Windows-Sysmon/Operational	13	Registry value set (rule: RegistryEvent)	Registry value set. • **EventType**: Process type (SetValue) • **Image**: Path to the executable file (C:\Windows\System32\svchost.exe) • **Details**: Setting value written to the registry (Sysinternals Sdelete) • **TargetObject**: Registry value at the write destination (\REGISTRY\A\[GUID]\Root\File\[GUID]\30000191d0\0)
	Microsoft-Windows-Sysmon/Operational	13	Registry value set (rule: RegistryEvent)	Registry value set. • **EventType**: Process type (SetValue) • **Image**: Path to the executable file (C:\Windows\System32\svchost.exe) • **Details**: Setting value written to the registry (Sysinternals - www.sysinternals.com) • **TargetObject**: Registry value at the write destination (\REGISTRY\A\[GUID]\Root\File\[GUID]\30000191d0\1)
3	Microsoft-Windows-Sysmon/Operational	13	Registry value set (rule: RegistryEvent)	Registry value set. • **EventType**: Process type (SetValue) • **Image**: Path to the executable file (C:\Windows\Explorer.EXE) • **Details**: Setting value written to the registry (Binary Data) • **TargetObject**: Registry value at the write destination (\REGISTRY\USER\[User SID]\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{[GUID]}\Count\[ROT13 of Path to Tool]\[ROT13 of Tool Executable File Name])
4	Microsoft-Windows-Sysmon/Operational	12	Registry object added or deleted (rule: RegistryEvent)	Registry object added or deleted. • **EventType**: Process type (CreateKey) • **Image**: Path to the executable file (path to the tool) • **TargetObject**: Created/deleted registry key/value (\REGISTRY\USER\[User SID]\SOFTWARE)
	Microsoft-Windows-Sysmon/Operational	12	Registry object added or deleted (rule: RegistryEvent)	Registry object added or deleted. • **EventType**: Process type (CreateKey) • **Image**: Path to the executable file (path to the tool) • **TargetObject**: Created/deleted registry key/value (\REGISTRY\USER\[User SID]\SOFTWARE\Sysinternals)
	Microsoft-Windows-Sysmon/Operational	12	Registry object added or deleted (rule: RegistryEvent)	Registry object added or deleted. • **EventType**: Process type (CreateKey) • **Image**: Path to the executable file (path to the tool) • **TargetObject**: Created/deleted registry key/value (\REGISTRY\USER\[User SID]\SOFTWARE\Sysinternals\SDelete)
5	Security	4656	File System/Other Object Access Events	A handle to an object was requested. • **Access Request Information > Access/Reason for Access/Access Mask**: Requested privileges (WriteData or AddFile, AppendData) • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of the user who executed the tool • **Subject > Logon ID**: Session ID of the user who executed the process • **Object > Handle ID**: ID of the relevant handle • **Object > Object Name**: Target file name (file to be deleted) **Remarks**: In the course of overwriting and deleting a file, **sdelete** creates a file. Some letters are added to the original file name. Deletion operation is repeatedly performed onto the file. For example, if the file to be deleted is "sdelete.txt", its file name may be "sdeleAAAAAAAAAAAAAAAAAAA.AAA", "sdeleZZZZZZZZZZZZZZZZZZZ.ZZZ", and so on. The letters and the number of overwriting operations differ depending on the specified number of deletion operations.

	Security	4658	File System	The handle to an object was closed. • **Process Information > Process ID**: Process ID (hexadecimal) • **Process Information > Process Name**: Name of the process that requested the object (path to the tool) • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of the user who executed the tool • **Subject > Logon ID**: Session ID of the user who executed the process • **Object > Handle ID**: ID of the relevant handle (handle obtained with the immediately prior Event ID: 4656)
6	Security	4656	File System/Other Object Access Events	A handle to an object was requested. • **Process Information > Process ID**: Process ID (hexadecimal) • **Access Request Information > Access/Reason for Access/Access Mask**: Requested privilege (DELETE) • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of the user who executed the tool • **Object > Object Name**: Target file name (file to be deleted) • **Process Information > Process Name**: Name of the process that closed the handle (path to the tool) • **Subject > Logon ID**: Session ID of the user who executed the process • **Object > Handle ID**: ID of the relevant handle
	Security	4663	File System	An attempt was made to access an object. • **Process Information > Process ID**: Process ID (hexadecimal) • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of the user who executed the tool • **Object > Object Name**: Target file name (file to be deleted) • **Process Information > Process Name**: Name of the process that closed the handle (path to the tool) • **Subject > Logon ID**: Session ID of the user who executed the process • **Object > Handle ID**: ID of the relevant handle (handle obtained with the immediately prior Event ID: 4656)
	Security	4660	File System	An object was deleted. • **Process Information > Process ID**: Process ID (hexadecimal) • **Process Information > Process Name**: Name of the process that closed the handle (path to the tool) • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of the user who executed the tool • **Object > Handle ID**: ID of the relevant handle (handle obtained with the immediately prior Event ID: 4656)
	Security	4658	File System	The handle to an object was closed. • **Process Information > Process ID**: Process ID (hexadecimal) • **Process Information > Process Name**: Name of the process that requested the object (path to the tool) • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of the user who executed the tool • **Object > Handle ID**: ID of the relevant handle (handle obtained with the immediately prior Event ID: 4656)
7	Security	4689	Process Termination	A process has exited. • **Process Information > Process ID**: Process ID (hexadecimal) • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of the user who executed the tool • **Process Information > Exit Status**: Process return value ("0x0" if the process exited normally) • **Process Information > Process Name**: Path to the executable file (path to the tool)
	Microsoft-Windows-Sysmon/Operational	5	Process terminated (rule: ProcessTerminate)	Process terminated. • **UtcTime**: Process terminated date and time (UTC) • **ProcessGuid/ProcessId**: Process ID • **Image**: Path to the executable file (path to the tool)
8	Microsoft-Windows-Sysmon/Operational	11	File created (rule: FileCreate)	File created.

			• **Image**: Path to the executable file (C:\Windows\System32\svchost.exe) • **TargetFilename**: Created file (C:\Windows\Prefetch\[Executable File Name of Tool]-[RANDOM].pf) • **CreationUtcTime**: File creation date and time (UTC)
Security	4656	File System/Other Object Access Events	A handle to an object was requested. • **Access Request Information > Access/Reason for Access/Access Mask**: Requested privileges (including WriteData or AddFile, and AppendData) • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of the user who executed the tool • **Object > Object Name**: Target file name (C:\Windows\Prefetch\[Executable File Name of Tool]-[RANDOM].pf) • **Process Information > Process Name**: Name of the process that closed the handle (C:\Windows\System32\svchost.exe) • **Object > Object Type**: Type of the file (File) • **Object > Handle ID**: ID of the relevant handle
Security	4663	File System	An attempt was made to access an object. • **Access Request Information > Access/Reason for Access/Access Mask**: Requested privileges (including WriteData or AddFile, and AppendData) • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of the user who executed the tool • **Object > Object Name**: Target file name (C:\Windows\Prefetch\[Executable File Name of Tool]-[RANDOM].pf) • **Process Information > Process Name**: Name of the process that closed the handle (C:\Windows\System32\svchost.exe) • **Object > Object Type**: Category of the target (File) • **Object > Handle ID**: ID of the relevant handle (handle requested in the immediately prior Event ID: 4656)
Security	4658	File System	The handle to an object was closed. • **Process Information > Process Name**: Name of the process that requested the object (C:\Windows\System32\svchost.exe) • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of the user who executed the tool • **Object > Handle ID**: ID of the relevant handle (handle requested in the immediately prior Event ID: 4656)

- UserAssist

#	Registry entry	Information That Can Be Confirmed
1	\REGISTRY\USER\[User SID]\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{[GUID]}\Count\[ROT13 of Path to Tool]\[ROT13 of Tool Executable File Name]	Date and time of the initial execution, Total number of executions

- MFT

#	Path	Header Flag	Validity
1	[Drive Name]:\Windows\Prefetch\[Executable File Name of Tool]-[RANDOM].pf	FILE	ALLOCATED
2	[File to be Deleted]	-	- (to be deleted)

- Prefetch

#	Prefetch File	Process Name	Process Path	Information That Can Be Confirmed

1	[Executable File Name of Tool]-[RANDOM].pf	[Executable File Name of Tool]	\VOLUME{[GUID]}\[Path to the Tool]	Last Run Time (last execution date and time)

- Registry Entry

#	Path	Type	Value
1	HKEY_USERS\[User SID]\SOFTwARE\Sysinternals\SDelete\EulaAccepted	DWORD	0x00000001
2	HKEY_USERS\[User SID]\SOFTwARE\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{[GUID]}\Count\[ROT13 of Path to Tool]\[ROT13 of Tool Executable File Name]	Binary	[Binary Value]