Quarks PWDump

- Table of Contents

Open all sections | Close all sections

- Tool Overview

Category

Password and Hash Dump

Description

Acquires the password hashes of domain and local accounts as well as cached passwords. NTDS.DIT files can be specified and analyzed.

Example of Presumed Tool Use During an Attack

This tool is used to log on to other hosts using acquired password.

- Tool Operation Overview

Item	Description
OS	Windows
Belonging to Domain	Not required
Rights	Administrator

- Information Acquired from Log

Standard Settings

- Host
  - Execution history (Prefetch)

Additional Settings

- Host
  - Execution history (audit policy, Sysmon)
  - Creation of a temporary file ("SAM-[RANDOM].dmp") (audit policy, Sysmon)

- Evidence That Can Be Confirmed When Execution is Successful

- A temporary file ("SAM-[RANDOM].dmp") was created and deleted.

- Main Information Recorded at Execution

- Host

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 ([Path to Tool] [Option]) • **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	4663	File System	An attempt was made to access an object. • **Access Request Information > Access/Reason for Access/Access Mask**: Requested privilege • **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 ([Temporary Folder]\SAM-[RANDOM].dmp and related files)

USN journal

#	File Name	Process
1	SAM-[RANDOM].dmp	CLOSE+FILE_DELETE
2	SAM-[RANDOM].dmp.LOG[NUM]	CLOSE+DATA_EXTEND+DATA_OVERWRITE+FILE_CREATE
3	SAM-[RANDOM].dmp{[GUID]}.TM.blf	DATA_EXTEND+DATA_OVERWRITE+FILE_CREATE
4	SAM-[RANDOM].dmp{[GUID]}.TMContainer[NUM].regtrans-ms	CLOSE+DATA_EXTEND+DATA_OVERWRITE+FILE_CREATE

MFT

#	Path	Header Flag	Validity
1	[Drive Name]:\Users\[User Name]\AppData\Local\Temp\SAM-[NUM].dmp.LOG[NUM]	FILE	ALLOCATED
2	[Drive Name]:\Users\[User Name]\AppData\Local\Temp\SAM-[NUM].dmp{[GUID]}.TM.blf	FILE	ALLOCATED
3	[Drive Name]:\Users\[User Name]\AppData\Local\Temp\SAM-[NUM].dmp{[GUID]}.TMContainer[NUM].regtrans-ms	FILE	ALLOCATED

Prefetch

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

- Details: Host

- 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 • **CurrentDirectory**: Work directory • **CommandLine**: Command line of the execution command ([Path to Tool] [Option]) • **IntegrityLevel**: Privilege level • **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 • **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 parent process that created the new process • **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 (2) • **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 (path to the tool) • **ProcessGuid/ProcessId**: Process ID • **TargetObject**: Created/deleted registry key/value (\REGISTRY\MACHINE\SYSTEM\ControlSet001\Control\Lsa)
	Security	4703	Token Right Adjusted Events	A token right was adjusted. • **Disabled Privileges**: Privileges that were disabled • **Target Account > Security ID/Account Name/Account Domain**: Target user SID/Account name/Domain • **Target Account > Logon ID**: Session ID of the target user • **Enabled Privileges**: Enabled privileges (SeRestorePrivilege) • **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 • **Process Information > Process ID**: ID of the executed process • **Process Information > Process Name**: Name of the process executed (path to the tool)
3	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) • **ProcessGuid/ProcessId**: Process ID • **TargetObject**: Created/deleted registry key/value (\REGISTRY\MACHINE\SECURITY)
	Security	4703	Token Right Adjusted Events	A token right was adjusted. • **Disabled Privileges**: Privileges that were disabled • **Target Account > Security ID/Account Name/Account Domain**: Target user SID/Account name/Domain • **Target Account > Logon ID**: Session ID of the target user • **Enabled Privileges**: Enabled privileges (SeBackupPrivilege) • **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 • **Process Information > Process ID**: ID of the executed process • **Process Information > Process Name**: Name of the process executed (path to the tool)
4	Microsoft-Windows-Sysmon/Operational	11	File created (rule: FileCreate)	File created. • **Image**: Path to the executable file (path to the tool) • **ProcessGuid/ProcessId**: Process ID • **TargetFilename**: Created file ([Temporary Folder]\SAM-[RANDOM].dmp) • **CreationUtcTime**: File creation date and time (UTC)
	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 • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of the user who executed the tool • **Object > Object Name**: Target file name ([Temporary Folder]\SAM-[RANDOM].dmp) • **Process Information > Process Name**: Name of the process that closed the handle (path to the tool) • **Object > Object Type**: Type of the file (File) • **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)

				• **Access Request Information > Access/Reason for Access/Access Mask**: Requested privilege • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of the user who executed the tool • **Object > Object Name**: Target file name ([Temporary Folder]\SAM-[RANDOM].dmp) • **Audit Success**: Success or failure (access successful) • **Process Information > Process Name**: Name of the process that closed the handle (path to the tool) • **Object > Object Type**: Category of the target (File) • **Subject > Logon ID**: Session ID of the user who executed the process • **Object > Handle ID**: ID of the relevant handle (handle obtained with Event ID: 4690)
	Security	4660	File System	An object was deleted. • **Process Information > Process ID**: Process ID (hexadecimal) • **Audit Success**: Success or failure (access successful) • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of the user who executed the tool • **Object > Object Name**: Target file name • **Access Request Information > Access**: Requested privilege • **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 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 • **Subject > Logon ID**: Session ID of the user who executed the process • **Object > Handle ID**: ID of the relevant handle (handle obtained with Event ID 4690)
5	Microsoft-Windows-Sysmon/Operational	11	File created (rule: FileCreate)	File created. • **Image**: Path to the executable file (path to the tool) • **ProcessGuid/ProcessId**: Process ID • **TargetFilename**: Created file ([Temporary Folder]\SAM-[RANDOM].dmp.LOG[NUM]) • **CreationUtcTime**: File creation date and time (UTC)
	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 • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of the user who executed the tool • **Object > Object Name**: Target file name ([Temporary Folder]\SAM-[RANDOM].dmp.LOG[NUM]) • **Process Information > Process Name**: Name of the process that closed the handle (path to the tool) • **Object > Object Type**: Type of the file (File) • **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) • **Access Request Information > Access/Reason for Access/Access Mask**: Requested privilege • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of the user who executed the tool • **Object > Object Name**: Target file name ([Temporary Folder]\SAM-[RANDOM].dmp.LOG[NUM]) • **Audit Success**: Success or failure (access successful) • **Process Information > Process Name**: Name of the process that closed the handle (path to the tool) • **Object > Object Type**: Category of the target (File) • **Subject > Logon ID**: Session ID of the user who executed the process • **Object > Handle ID**: ID of the relevant handle (handle obtained with Event ID: 4690)
	Security	4660	File System	An object was deleted.

				• **Process Information > Process ID**: Process ID (hexadecimal) • **Audit Success**: Success or failure (access successful) • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of the user who executed the tool • **Object > Object Name**: Target file name • **Access Request Information > Access**: Requested privilege • **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 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 • **Subject > Logon ID**: Session ID of the user who executed the process • **Object > Handle ID**: ID of the relevant handle (handle obtained with Event ID 4690)
6	Microsoft-Windows-Sysmon/Operational	11	File created (rule: FileCreate)	File created. • **Image**: Path to the executable file (path to the tool) • **ProcessGuid/ProcessId**: Process ID • **TargetFilename**: Created file ([Temporary Folder]\SAM-[RANDOM].dmp{[GUID]}.TM.blf) • **CreationUtcTime**: File creation date and time (UTC)
	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 • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of the user who executed the tool • **Object > Object Name**: Target file name ([Temporary Folder]\SAM-[RANDOM].dmp{[GUID]}.TM.blf) • **Process Information > Process Name**: Name of the process that closed the handle (path to the tool) • **Object > Object Type**: Type of the file (File) • **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) • **Access Request Information > Access/Reason for Access/Access Mask**: Requested privilege • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of the user who executed the tool • **Object > Object Name**: Target file name ([Temporary Folder]\SAM-[RANDOM].dmp{[GUID]}.TM.blf) • **Audit Success**: Success or failure (access successful) • **Process Information > Process Name**: Name of the process that closed the handle (path to the tool) • **Object > Object Type**: Category of the target (File) • **Subject > Logon ID**: Session ID of the user who executed the process • **Object > Handle ID**: ID of the relevant handle (handle obtained with Event ID: 4690)
	Security	4660	File System	An object was deleted. • **Process Information > Process ID**: Process ID (hexadecimal) • **Audit Success**: Success or failure (access successful) • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of the user who executed the tool • **Object > Object Name**: Target file name • **Access Request Information > Access**: Requested privilege • **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 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 • **Subject > Logon ID**: Session ID of the user who executed the process • **Object > Handle ID**: ID of the relevant handle (handle obtained with Event ID 4690)
7	Microsoft-Windows-Sysmon/Operational	11	File created (rule: FileCreate)	File created. • **Image**: Path to the executable file (path to the tool) • **ProcessGuid/ProcessId**: Process ID • **TargetFilename**: Created file ([Temporary Folder]\SAM-[RANDOM].dmp{[GUID]}.TMContainer[NUM].regtrans-ms) • **CreationUtcTime**: File creation date and time (UTC)
	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 • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of the user who executed the tool • **Object > Object Name**: Target file name ([Temporary Folder]\SAM-[RANDOM].dmp{[GUID]}.TMContainer[NUM].regtrans-ms) • **Process Information > Process Name**: Name of the process that closed the handle (path to the tool) • **Object > Object Type**: Type of the file (File) • **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) • **Access Request Information > Access/Reason for Access/Access Mask**: Requested privilege • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of the user who executed the tool • **Object > Object Name**: Target file name ([Temporary Folder]\SAM-[RANDOM].dmp{[GUID]}.TMContainer[NUM].regtrans-ms) • **Audit Success**: Success or failure (access successful) • **Process Information > Process Name**: Name of the process that closed the handle (path to the tool) • **Object > Object Type**: Category of the target (File) • **Subject > Logon ID**: Session ID of the user who executed the process • **Object > Handle ID**: ID of the relevant handle (handle obtained with Event ID: 4690)
	Security	4660	File System	An object was deleted. • **Process Information > Process ID**: Process ID (hexadecimal) • **Audit Success**: Success or failure (access successful) • **Subject > Security ID/Account Name/Account Domain**: SID/Account name/Domain of the user who executed the tool • **Object > Object Name**: Target file name • **Access Request Information > Access**: Requested privilege • **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 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 • **Subject > Logon ID**: Session ID of the user who executed the process • **Object > Handle ID**: ID of the relevant handle (handle obtained with Event ID 4690)
8	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) • **ProcessGuid/ProcessId**: Process ID • **TargetObject**: Created/deleted registry key/value (under \REGISTRY\MACHINE\QUARKS-SAM)

9	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)
	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) • **Log Date and Time**: Process terminated date and time (local time) • **Process Information > Process Name**: Path to the executable file (path to the tool) • **Subject > Logon ID**: Session ID of the user who executed the process
10	Microsoft-Windows-Sysmon/Operational	11	File created (rule: FileCreate)	File created. • **Image**: Path to the executable file (C:\Windows\System32\svchost.exe) • **ProcessGuid/ProcessId**: Process ID • **TargetFilename**: Created file (C:\Windows\Prefetch\[Executable File 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. • **Process Information > Process ID**: Process ID (hexadecimal) • **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 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) • **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) • **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 (C:\Windows\Prefetch\[Executable File of Tool]-[RANDOM].pf) • **Audit Success**: Success or failure (access successful) • **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) • **Subject > Logon ID**: Session ID of the user who executed the process • **Object > Handle ID**: ID of the relevant handle (handle obtained with 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 (C:\Windows\System32\svchost.exe) • **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 Event ID 4656)

- USN Journal

#	File Name	Process	Attribute
1	SAM-[RANDOM].dmp	FILE_CREATE	archive
	SAM-[RANDOM].dmp	DATA_EXTEND+FILE_CREATE	archive
	SAM-[RANDOM].dmp	DATA_EXTEND+DATA_OVERWRITE+FILE_CREATE	archive
	SAM-[RANDOM].dmp	CLOSE+DATA_EXTEND+DATA_OVERWRITE+FILE_CREATE	archive

2	SAM-[RANDOM].dmp.LOG[NUM]	FILE_CREATE	archive
	SAM-[RANDOM].dmp.LOG[NUM]	DATA_EXTEND+FILE_CREATE	archive
	SAM-[RANDOM].dmp.LOG[NUM]	DATA_EXTEND+DATA_OVERWRITE+FILE_CREATE	archive
	SAM-[RANDOM].dmp.LOG[NUM]	CLOSE+DATA_EXTEND+DATA_OVERWRITE+FILE_CREATE	archive
3	SAM-[RANDOM].dmp{[GUID]}.TM.blf	FILE_CREATE	archive
	SAM-[RANDOM].dmp{[GUID]}.TM.blf	DATA_EXTEND+FILE_CREATE	archive
	SAM-[RANDOM].dmp{[GUID]}.TM.blf	DATA_EXTEND+DATA_OVERWRITE+FILE_CREATE	archive
4	SAM-[RANDOM].dmp{[GUID]}.TMContainer[NUM].regtrans-ms	FILE_CREATE	hidden+system+archive
	SAM-[RANDOM].dmp{[GUID]}.TMContainer[NUM].regtrans-ms	DATA_EXTEND+FILE_CREATE	hidden+system+archive
	SAM-[RANDOM].dmp{[GUID]}.TMContainer[NUM].regtrans-ms	DATA_EXTEND+DATA_OVERWRITE+FILE_CREATE	hidden+system+archive
	SAM-[RANDOM].dmp{[GUID]}.TMContainer[NUM].regtrans-ms	CLOSE+DATA_EXTEND+DATA_OVERWRITE+FILE_CREATE	hidden+system+archive
5	SAM-[RANDOM].dmp	DATA_EXTEND	archive
	SAM-[RANDOM].dmp	DATA_EXTEND+DATA_OVERWRITE	archive
	SAM-[RANDOM].dmp	BASIC_INFO_CHANGE+DATA_EXTEND+DATA_OVERWRITE	archive
	SAM-[RANDOM].dmp	BASIC_INFO_CHANGE+CLOSE+DATA_EXTEND+DATA_OVERWRITE	archive
	SAM-[RANDOM].dmp	CLOSE+FILE_DELETE	archive
6	[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

- MFT

#	Path	Header Flag	Validity
1	[Drive Name]:\Users\[User Name]\AppData\Local\Temp\SAM-[NUM].dmp.LOG[NUM]	FILE	ALLOCATED
2	[Drive Name]:\Users\[User Name]\AppData\Local\Temp\SAM-[NUM].dmp{[GUID]}.TM.blf	FILE	ALLOCATED
3	[Drive Name]:\Users\[User Name]\AppData\Local\Temp\SAM-[NUM].dmp{[GUID]}.TMContainer[NUM].regtrans-ms	FILE	ALLOCATED
4	[Drive Name]:\Windows\Prefetch\[Executable File Name of Tool]-[RANDOM].pf	FILE	ALLOCATED

- Prefetch

#	Prefetch File	Process Name	Process Path	Information That Can Be Confirmed
1	C:\Windows\Prefetch\[Executable File Name of Tool]-[RANDOM].pf	[Executable File Name of Tool]	[Path to Tool]	Last Run Time (last execution date and time)

- Remarks

- The command line option "-dhdc" was used in this research.