

WCE

-

Table of Contents

- [Tool Overview](#)
- [Tool Operation Overview](#)
- [Information Acquired from Log](#)
- [Evidence That Can Be Confirmed When Execution is Successful](#)
- [Main Information Recorded at Execution](#)
- [Details: Host](#)
- [Remarks](#)

[Open all sections](#) | [Close all sections](#)

-

Tool Overview

Category

Password and Hash Dump

Description

Acquires a password hash in the memory of a host.

Example of Presumed Tool Use During an Attack

This tool uses the acquired password hash to perform attacks such as pass-the-hash.

-

Tool Operation Overview

Item	Description
OS	Windows 7 32-bit version
Belonging to Domain	Not required
Rights	Administrator

-

Information Acquired from Log

Standard Settings

- Host
 - Execution history (Prefetch)
 - Creation of a temporary file (wceaux.dll) (audit policy, USN journal)

Additional Settings

- Host
 - Execution history (audit policy, Sysmon)
 - Reference of lsass.exe by WCE (Sysmon)
 - Creation/deletion of a file (audit policy)

-

Evidence That Can Be Confirmed When Execution is Successful

- The "C:\Users\[User Name]\AppData\Local\Temp\wceaux.dll" file 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)	<div>Process Create.</div> <ul style="list-style-type: none">CommandLine: Command line of the execution command ([Path to Tool] -w)UtcTime: Process execution date and time (UTC)ProcessGuid/ProcessId: Process IDImage: Path to the executable file (path to the tool)User: Execute as user
2	Microsoft-Windows-Sysmon/Operational	10	Process accessed (rule: ProcessAccess)	<div>Process accessed.</div> <ul style="list-style-type: none">SourceProcessGUID/SourceProcessId/SourceThreadId: Process of the access source process/Thread IDTargetProcessGUID/TargetProcessId: Process ID of the access destination processGrantedAccess: Details of the granted accessSourceImage: Path to the access source process (path to the tool)TargetImage: Path to the access destination process (C:\Windows\system32\lsass.exe)
3	Security	4663	File System	<div>An attempt was made to access an object.</div> <ul style="list-style-type: none">Access Request Information > Access/Reason for Access/Access Mask: Requested privileges (WriteData or AddFile)Subject > Security ID/Account Name/Account Domain: SID/Account name/Domain of the user who executed the toolProcess Information > Process Name: Name of the process that closed the handle (path to the tool)Object > Object Name: Target file name (C:\Users\[User Name]\AppData\Local\Temp\wceaux.dll)
4	Security	4663	File System	<div>An attempt was made to access an object.</div> <ul style="list-style-type: none">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 toolObject > Object Name: Target file name (C:\Users\[User Name]\AppData\Local\Temp\wceaux.dll)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 processObject > Handle ID: ID of the relevant handle (handle obtained with Event ID 4656)

5	Microsoft-Windows-Sysmon/Operational	8	CreateRemoteThread detected (rule: CreateRemoteThread)	CreateRemoteThread detected. <ul style="list-style-type: none">• NewThreadId: Thread ID of the new thread• TargetProcessGuid/TargetProcessId: Process ID of the destination process• TargetImage: Path to the creation destination process (C:\Windows\System32\lsass.exe)• UtcTime: Execution date and time (UTC)• SourceImage: Path to the source process (path to the tool)• SourceProcessGuid/SourceProcessId: Process ID of the source process
---	--------------------------------------	---	--	--

USN journal

#	File Name	Process
1	wceaux.dll	CLOSE+FILE_DELETE

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. <ul style="list-style-type: none">• 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] -w)• IntegrityLevel: Privilege level (High)• 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. (path to the tool) <ul style="list-style-type: none">• 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 (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

				<div>Process ID" in Windows 7</div> <ul style="list-style-type: none">• Subject > Logon ID: Session ID of the user who executed the process
2	Microsoft-Windows-Sysmon/Operational	11	File created (rule: FileCreate)	<div>File created.</div> <ul style="list-style-type: none">• Image: Path to the executable file (path to the tool)• ProcessGuid/ProcessId: Process ID• TargetFilename: Created file (C:\Users\[User Name]\AppData\Local\Temp\wceaux.dll)• CreationUtcTime: File creation date and time (UTC)
	Security	4656	File System/Other Object Access Events	<div>A handle to an object was requested.</div> <ul style="list-style-type: none">• 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 (C:\Users\[User Name]\AppData\Local\Temp\wceaux.dll)• 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	<div>An attempt was made to access an object.</div> <ul style="list-style-type: none">• Process Information > Process ID: Process ID (hexadecimal)• Access Request Information > Access/Reason for Access/Access Mask: Requested privileges (WriteData or AddFile)• 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:\Users\[User Name]\AppData\Local\Temp\wceaux.dll)• 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 4656)
	Security	4658	File System	<div>The handle to an object was closed.</div> <ul style="list-style-type: none">• 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 4656)
3	Microsoft-Windows-Sysmon/Operational	10	Process accessed (rule: ProcessAccess)	<div>Process accessed.</div> <ul style="list-style-type: none">• SourceProcessGUID/SourceProcessId/SourceThreadId: Process of the access source process/Thread ID• TargetProcessGUID/TargetProcessId: Process ID of the access destination process

				<ul style="list-style-type: none">• GrantedAccess: Details of the granted access• SourceImage: Path to the access source process (path to the tool)• TargetImage: Path to the access destination process (C:\Windows\system32\lsass.exe)
	Microsoft-Windows-Sysmon/Operational	8	CreateRemoteThread detected (rule: CreateRemoteThread)	CreateRemoteThread detected. <ul style="list-style-type: none">• NewThreadId: Thread ID of the new thread• TargetProcessGuid/TargetProcessId: Process ID of the destination process• TargetImage: Path to the creation destination process (C:\Windows\System32\lsass.exe)• UtcTime: Execution date and time (UTC)• SourceImage: Path to the source process (path to the tool)• SourceProcessGuid/SourceProcessId: Process ID of the source process
	Microsoft-Windows-Sysmon/Operational	10	Process accessed (rule: ProcessAccess)	Process accessed. <ul style="list-style-type: none">• SourceProcessGUID/SourceProcessId/SourceThreadId: Process of the access source process/Thread ID• TargetProcessGUID/TargetProcessId: Process ID of the access destination process• GrantedAccess: Details of the granted access• SourceImage: Path to the access source process (path to the tool)• TargetImage: Path to the access destination process (C:\Windows\system32\lsass.exe)
4	Security	4656	File System/Other Object Access Events	A handle to an object was requested. <ul style="list-style-type: none">• Process Information > Process ID: Process ID (hexadecimal)• Access Request Information > Access/Reason for Access/Access Mask: Requested privilege (including 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 (C:\Users\[User Name]\AppData\Local\Temp\wceaux.dll)• 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. <ul style="list-style-type: none">• 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 (C:\Users\[User Name]\AppData\Local\Temp\wceaux.dll)• 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 4656)
	Security	4660	File System	An object was deleted.

				<ul style="list-style-type: none">• 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	<p>The handle to an object was closed.</p> <ul style="list-style-type: none">• 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 4656)
6	Microsoft-Windows-Sysmon/Operational	5	Process terminated (rule: ProcessTerminate)	<p>Process terminated.</p> <ul style="list-style-type: none">• 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	<p>A process has exited.</p> <ul style="list-style-type: none">• 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• 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

-

USN Journal

#	File Name	Process	Attribute
1	wceaux.dll	FILE_CREATE	archive+not_indexed
	wceaux.dll	DATA_EXTEND+FILE_CREATE	archive+not_indexed
	wceaux.dll	CLOSE+DATA_EXTEND+FILE_CREATE	archive+not_indexed
2	wceaux.dll	DATA_OVERWRITE	archive+not_indexed
	wceaux.dll	CLOSE+DATA_OVERWRITE	archive+not_indexed
	wceaux.dll	CLOSE+FILE_DELETE	archive+not_indexed
3	[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]:\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

- If Windows 10 abnormally terminates, the Event ID: 1001 (APPCRASH) is recorded in the event log "Application". In addition, a crash report is created under "C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_[Tool Name]_[RANDOM]". If this file remains, there is a possibility that the status can be investigated. Furthermore, since a crash report list is managed in the registry, "AppCrash_[Tool Name]_[RANDOM]" may be recorded under "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Windows Error Reporting\Debug\StoreLocation" and "HKEY_USERS\[User SID]\Software\Microsoft\Windows\Windows Error Reporting\Debug\StoreLocation".
- If Windows 10 abnormally terminates, there is a possibility that "C:\Users\[User Name]\AppData\Local\Temp\wceaux.dll" remains without being deleted. Even if the file is deleted, the event is recorded in an event log and USN journal.