OPERATIONS DEBRIEF

Generated on 2026-03-17T23:48:38Z

This document covers the overall campaign analytics made up of the selected set of operations. The below sections contain general metadata about the selected operations as well as graphical views of the operations, the techniques and tactics used, and the facts discovered by the operations. The following sections include a more in depth review of each specific operation ran.

Operations: SMB Lateral Movement Campaign
Agents: 2 **Steps:** 14

STATISTICS

An operation's planner makes up the decision making process. It contains logic for how a running operation should make decisions about which abilities to use and in what order. An objective is a collection of fact targets, called goals, which can be tied to adversaries. During the course of an operation, every time the planner is evaluated, the current objective status is evaluated in light of the current knowledge of the operation, with the operation completing should all goals be met.

Metric	Value
Operations	1
Total Steps	14
Steps by Status	14 success
Unique Agents	2
Unique Tactics	9
Unique Techniques	14

Name	State	Planner	Objective	Time
SMB Lateral Movement Campaign	finished	atomic	default	2026-03-17T23:48:37Z

AGENTS

The table below displays information about the agents used. An agent's paw is the unique identifier, or paw print, of an agent. Also included are the username of the user who executed the agent, the privilege level of the agent process, and the name of the agent executable.

Paw	Host	Platform	Group	Username	Privilege	Arch	Executable
smbpaw01	WORKSTATION-01	windows	red	CORP\admin	Elevated		sandcat.exe
smbpaw02	web-server-01	linux	red	root	Elevated		sandcat

TACTICS AND TECHNIQUES

Tactics	Techniques	Abilities	Detections
Collection	T1560.001: Archive via Utility	Archive via Utility (T1560.001)	DET0298
Command-And-Control	T1071.001: Web Protocols T1105: Ingress Tool Transfer	Web Protocols (T1071.001) Ingress Tool Transfer (T1105)	DET0027 DET0060
Credential-Access	T1003.001: LSASS Memory	LSASS Memory (T1003.001)	DET0363
Defense-Evasion	T1055.001: Dynamic-link Library Injection T1070.004: File Deletion T1036.005: Match Legitimate Name or Location	Dynamic-link Library Injection (T1055.001) File Deletion (T1070.004) Match Legitimate Name or Location (T1036.005)	DET0389 DET0140 DET0347
Discovery	T1083: File and Directory Discovery	File and Directory Discovery (T1083)	DET0370
Execution	T1059.001: PowerShell T1053.005: Scheduled Task	PowerShell (T1059.001) Scheduled Task (T1053.005)	DET0455 DET0441
Lateral-Movement	T1021.002: SMB/Windows Admin Shares T1021.001: Remote Desktop Protocol	SMB/Windows Admin Shares (T1021.002) Remote Desktop Protocol (T1021.001)	DET0530 DET0327
Persistence	T1547.001: Registry Run Keys / Startup Folder	Registry Run Keys / Startup Folder (T1547.001)	DET0365
Privilege-Escalation	T1548.001: Setuid and Setgid	Setuid and Setgid (T1548.001)	DET0110

STEPS IN OPERATION SMB LATERAL MOVEMENT CAMPAIGN

The table below shows detailed information about the steps taken in an operation and whether the command run discovered any facts.

Time	Status	Agent	Tactic	Technique	Name	Command	Facts
2026-03-17T23:48:37Z	success	smbpaw01	discovery	File and Directory Discovery	File and Directory Discovery (T1083)	File and Directory Discovery (T1083) executed on windows	Yes

Time	Status	Agent	Tactic	Technique	Name	Command	Facts
2026-03-17T23:48:37Z	success	smbpaw01	persistence	Registry Run Keys / Startup Folder	Registry Run Keys / Startup Folder (T1547.001)	Registry Run Keys / Startup Folder (T1547.001) executed on windows	No
2026-03-17T23:48:37Z	success	smbpaw01	collection	Archive via Utility	Archive via Utility (T1560.001)	Archive via Utility (T1560.001) executed on windows	No
2026-03-17T23:48:37Z	success	smbpaw02	privilege-escalation	Setuid and Setgid	Setuid and Setgid (T1548.001)	Setuid and Setgid (T1548.001) executed on linux	No
2026-03-17T23:48:37Z	success	smbpaw01	execution	PowerShell	PowerShell (T1059.001)	PowerShell (T1059.001) executed on windows	No
2026-03-17T23:48:37Z	success	smbpaw01	execution	Scheduled Task	Scheduled Task (T1053.005)	Scheduled Task (T1053.005) executed on windows	No
2026-03-17T23:48:37Z	success	smbpaw01	lateral-movement	SMB/Windows Admin Shares	SMB/Windows Admin Shares (T1021.002)	SMB/Windows Admin Shares (T1021.002) executed on windows	Yes
2026-03-17T23:48:37Z	success	smbpaw01	lateral-movement	Remote Desktop Protocol	Remote Desktop Protocol (T1021.001)	Remote Desktop Protocol (T1021.001) executed on windows	No
2026-03-17T23:48:37Z	success	smbpaw01	defense-evasion	Dynamic-link Library Injection	Dynamic-link Library Injection (T1055.001)	Dynamic-link Library Injection (T1055.001) executed on windows	No
2026-03-17T23:48:37Z	success	smbpaw01	credential-access	LSASS Memory	LSASS Memory (T1003.001)	LSASS Memory (T1003.001) executed on windows	Yes
2026-03-17T23:48:37Z	success	smbpaw01	defense-evasion	File Deletion	File Deletion (T1070.004)	File Deletion (T1070.004) executed on windows	No
2026-03-17T23:48:37Z	success	smbpaw01	command-and-control	Web Protocols	Web Protocols (T1071.001)	Web Protocols (T1071.001) executed on windows	No
2026-03-17T23:48:37Z	success	smbpaw01	defense-evasion	Match Legitimate Name or Location	Match Legitimate Name or Location (T1036.005)	Match Legitimate Name or Location (T1036.005) executed on windows	No

Time	Status	Agent	Tactic	Technique	Name	Command	Facts
2026-03-17T23:48:37Z	success	smbpaw01	command-and-control	Ingress Tool Transfer	Ingress Tool Transfer (T1105)	Ingress Tool Transfer (T1105) executed on windows	No

Detections for SMB Lateral Movement Campaign

This section lists mapping of Analytic Elements to Data Components and their tunable fields for the selected operation.

Detection Strategies

Detection Strategy ID (DET0363)

Detection Strategy Name (Detection of Credential Dumping from LSASS Memory via Access and Dump Sequence)

Analytic (AN1030 to AN1030)

Analytic Elements

AN	Platform	Detection Statement	Data Component Elements (DC)			Mutable Elements	
			Name	Channel	Data Component	Field	Description
AN1030	Windows	A non-privileged or abnormal process attempts to open a handle with full access (0x1F0FFF) to lsass.exe and subsequently invokes memory dump, file creation, or registry modification indicative of credential scraping. This behavior chain reflects staged credential theft activity.	WinEventLog:Sysmon	EventCode=10	Process Access	AccessMask	Set to 0x1F0FFF to detect full memory access attempts; can be scoped down to reduce noise.
AN1030	Windows	A non-privileged or abnormal process attempts to open a handle with full access (0x1F0FFF) to lsass.exe and subsequently invokes memory dump, file creation, or registry modification indicative of credential scraping. This behavior chain reflects staged credential theft activity.	WinEventLog:Sysmon	EventCode=10	Process Access	TimeWindow	Defines time between LSASS access and dump file creation or registry modification (e.g., 5 minutes).
AN1030	Windows	A non-privileged or abnormal process attempts to open a handle with full access (0x1F0FFF) to lsass.exe and subsequently invokes memory dump, file creation, or registry modification indicative of credential scraping. This behavior chain reflects staged credential theft activity.	WinEventLog:Sysmon	EventCode=10	Process Access	ParentProcessName	Allowlist known legitimate tools (e.g., AV/EDR) accessing lsass.exe.
AN1030	Windows	A non-privileged or abnormal process attempts to open a handle with full access (0x1F0FFF) to lsass.exe and subsequently invokes memory dump, file creation, or registry modification indicative of credential scraping. This behavior chain reflects staged credential theft activity.	WinEventLog:Sysmon	EventCode=10	Process Access	DumpFilePath	Paths where memory dumps are written, e.g., %TEMP%, C:\Windows\Temp.
AN1030	Windows	A non-privileged or abnormal process attempts to open a handle with full access (0x1F0FFF) to lsass.exe and subsequently invokes memory dump, file creation, or registry modification indicative of credential scraping. This behavior chain reflects staged credential theft activity.	WinEventLog:Sysmon	EventCode=10	Process Access	CommandLinePattern	Common dumping syntax like rundll32, procdump, comsvcs.dll, Invoke-Mimikatz.

AN	Platform	Detection Statement	Data Component Elements (DC)			Mutable Elements	
			Name	Channel	Data Component	Field	Description
AN1030	Windows	A non-privileged or abnormal process attempts to open a handle with full access (0x1F0FFF) to lsass.exe and subsequently invokes memory dump, file creation, or registry modification indicative of credential scraping. This behavior chain reflects staged credential theft activity.	WinEventLog:Sysmon	EventCode=1	Process Creation	AccessMask	Set to 0x1F0FFF to detect full memory access attempts; can be scoped down to reduce noise.
AN1030	Windows	A non-privileged or abnormal process attempts to open a handle with full access (0x1F0FFF) to lsass.exe and subsequently invokes memory dump, file creation, or registry modification indicative of credential scraping. This behavior chain reflects staged credential theft activity.	WinEventLog:Sysmon	EventCode=1	Process Creation	TimeWindow	Defines time between LSASS access and dump file creation or registry modification (e.g., 5 minutes).
AN1030	Windows	A non-privileged or abnormal process attempts to open a handle with full access (0x1F0FFF) to lsass.exe and subsequently invokes memory dump, file creation, or registry modification indicative of credential scraping. This behavior chain reflects staged credential theft activity.	WinEventLog:Sysmon	EventCode=1	Process Creation	ParentProcessName	Allowlist known legitimate tools (e.g., AV/EDR) accessing lsass.exe.
AN1030	Windows	A non-privileged or abnormal process attempts to open a handle with full access (0x1F0FFF) to lsass.exe and subsequently invokes memory dump, file creation, or registry modification indicative of credential scraping. This behavior chain reflects staged credential theft activity.	WinEventLog:Sysmon	EventCode=1	Process Creation	DumpFilePath	Paths where memory dumps are written, e.g., %TEMP%, C:\Windows\Temp.
AN1030	Windows	A non-privileged or abnormal process attempts to open a handle with full access (0x1F0FFF) to lsass.exe and subsequently invokes memory dump, file creation, or registry modification indicative of credential scraping. This behavior chain reflects staged credential theft activity.	WinEventLog:Sysmon	EventCode=1	Process Creation	CommandLinePattern	Common dumping syntax like rundll32, procdump, comsvcs.dll, Invoke-Mimikatz.
AN1030	Windows	A non-privileged or abnormal process attempts to open a handle with full access (0x1F0FFF) to lsass.exe and subsequently invokes memory dump, file creation, or registry modification indicative of credential scraping. This behavior chain reflects staged credential theft activity.	WinEventLog:Sysmon	EventCode=11	File Creation	AccessMask	Set to 0x1F0FFF to detect full memory access attempts; can be scoped down to reduce noise.

AN	Platform	Detection Statement	Data Component Elements (DC)			Mutable Elements	
			Name	Channel	Data Component	Field	Description
AN1030	Windows	A non-privileged or abnormal process attempts to open a handle with full access (0x1F0FFF) to lsass.exe and subsequently invokes memory dump, file creation, or registry modification indicative of credential scraping. This behavior chain reflects staged credential theft activity.	WinEventLog:Sysmon	EventCode=11	File Creation	TimeWindow	Defines time between LSASS access and dump file creation or registry modification (e.g., 5 minutes).
AN1030	Windows	A non-privileged or abnormal process attempts to open a handle with full access (0x1F0FFF) to lsass.exe and subsequently invokes memory dump, file creation, or registry modification indicative of credential scraping. This behavior chain reflects staged credential theft activity.	WinEventLog:Sysmon	EventCode=11	File Creation	ParentProcessName	Allowlist known legitimate tools (e.g., AV/EDR) accessing lsass.exe.
AN1030	Windows	A non-privileged or abnormal process attempts to open a handle with full access (0x1F0FFF) to lsass.exe and subsequently invokes memory dump, file creation, or registry modification indicative of credential scraping. This behavior chain reflects staged credential theft activity.	WinEventLog:Sysmon	EventCode=11	File Creation	DumpFilePath	Paths where memory dumps are written, e.g., %TEMP%, C:\Windows\Temp.
AN1030	Windows	A non-privileged or abnormal process attempts to open a handle with full access (0x1F0FFF) to lsass.exe and subsequently invokes memory dump, file creation, or registry modification indicative of credential scraping. This behavior chain reflects staged credential theft activity.	WinEventLog:Sysmon	EventCode=11	File Creation	CommandLinePattern	Common dumping syntax like rundll32, procdump, comsvcs.dll, Invoke-Mimikatz.
AN1030	Windows	A non-privileged or abnormal process attempts to open a handle with full access (0x1F0FFF) to lsass.exe and subsequently invokes memory dump, file creation, or registry modification indicative of credential scraping. This behavior chain reflects staged credential theft activity.	WinEventLog:Security	EventCode=4673	User Account Metadata	AccessMask	Set to 0x1F0FFF to detect full memory access attempts; can be scoped down to reduce noise.
AN1030	Windows	A non-privileged or abnormal process attempts to open a handle with full access (0x1F0FFF) to lsass.exe and subsequently invokes memory dump, file creation, or registry modification indicative of credential scraping. This behavior chain reflects staged credential theft activity.	WinEventLog:Security	EventCode=4673	User Account Metadata	TimeWindow	Defines time between LSASS access and dump file creation or registry modification (e.g., 5 minutes).

AN	Platform	Detection Statement	Data Component Elements (DC)			Mutable Elements	
			Name	Channel	Data Component	Field	Description
AN1030	Windows	A non-privileged or abnormal process attempts to open a handle with full access (0x1F0FFF) to lsass.exe and subsequently invokes memory dump, file creation, or registry modification indicative of credential scraping. This behavior chain reflects staged credential theft activity.	WinEventLog:Security	EventCode=4673	User Account Metadata	ParentProcessName	Allowlist known legitimate tools (e.g., AV/EDR) accessing lsass.exe.
AN1030	Windows	A non-privileged or abnormal process attempts to open a handle with full access (0x1F0FFF) to lsass.exe and subsequently invokes memory dump, file creation, or registry modification indicative of credential scraping. This behavior chain reflects staged credential theft activity.	WinEventLog:Security	EventCode=4673	User Account Metadata	DumpFilePath	Paths where memory dumps are written, e.g., %TEMP%, C:\Windows\Temp.
AN1030	Windows	A non-privileged or abnormal process attempts to open a handle with full access (0x1F0FFF) to lsass.exe and subsequently invokes memory dump, file creation, or registry modification indicative of credential scraping. This behavior chain reflects staged credential theft activity.	WinEventLog:Security	EventCode=4673	User Account Metadata	CommandLinePattern	Common dumping syntax like rundll32, procdump, comsvcs.dll, Invoke-Mimikatz.
AN1030	Windows	A non-privileged or abnormal process attempts to open a handle with full access (0x1F0FFF) to lsass.exe and subsequently invokes memory dump, file creation, or registry modification indicative of credential scraping. This behavior chain reflects staged credential theft activity.	WinEventLog:Sysmon	EventCode=13, 14	Windows Registry Key Modification	AccessMask	Set to 0x1F0FFF to detect full memory access attempts; can be scoped down to reduce noise.
AN1030	Windows	A non-privileged or abnormal process attempts to open a handle with full access (0x1F0FFF) to lsass.exe and subsequently invokes memory dump, file creation, or registry modification indicative of credential scraping. This behavior chain reflects staged credential theft activity.	WinEventLog:Sysmon	EventCode=13, 14	Windows Registry Key Modification	TimeWindow	Defines time between LSASS access and dump file creation or registry modification (e.g., 5 minutes).
AN1030	Windows	A non-privileged or abnormal process attempts to open a handle with full access (0x1F0FFF) to lsass.exe and subsequently invokes memory dump, file creation, or registry modification indicative of credential scraping. This behavior chain reflects staged credential theft activity.	WinEventLog:Sysmon	EventCode=13, 14	Windows Registry Key Modification	ParentProcessName	Allowlist known legitimate tools (e.g., AV/EDR) accessing lsass.exe.

AN	Platform	Detection Statement	Data Component Elements (DC)			Mutable Elements	
			Name	Channel	Data Component	Field	Description
AN1030	Windows	A non-privileged or abnormal process attempts to open a handle with full access (0x1F0FFF) to lsass.exe and subsequently invokes memory dump, file creation, or registry modification indicative of credential scraping. This behavior chain reflects staged credential theft activity.	WinEventLog:Sysmon	EventCode=13, 14	Windows Registry Key Modification	DumpFilePath	Paths where memory dumps are written, e.g., %TEMP%, C:\Windows\Temp.
AN1030	Windows	A non-privileged or abnormal process attempts to open a handle with full access (0x1F0FFF) to lsass.exe and subsequently invokes memory dump, file creation, or registry modification indicative of credential scraping. This behavior chain reflects staged credential theft activity.	WinEventLog:Sysmon	EventCode=13, 14	Windows Registry Key Modification	CommandLinePattern	Common dumping syntax like rundll32, procdump, comsvcs.dll, Invoke-Mimikatz.

Detection Strategies

Detection Strategy ID (DET0327)

Detection Strategy Name (Multi-event Detection Strategy for RDP-Based Remote Logins and Post-Access Activity)

Analytic (AN0931 to AN0931)

Analytic Elements

AN	Platform	Detection Statement	Data Component Elements (DC)			Mutable Elements	
			Name	Channel	Data Component	Field	Description
AN0931	Windows	Remote Desktop (RDP) logon by a user followed by unusual process execution, file access, or lateral movement activity within a short timeframe.	WinEventLog:Security	EventCode=4624, 4648	Logon Session Creation	TimeWindow	Temporal threshold to correlate login with post-login activity (e.g., 5 minutes)
AN0931	Windows	Remote Desktop (RDP) logon by a user followed by unusual process execution, file access, or lateral movement activity within a short timeframe.	WinEventLog:Security	EventCode=4624, 4648	Logon Session Creation	UserContext	Tune for non-admin users or service accounts expected to use RDP
AN0931	Windows	Remote Desktop (RDP) logon by a user followed by unusual process execution, file access, or lateral movement activity within a short timeframe.	WinEventLog:Security	EventCode=4624, 4648	Logon Session Creation	ProcessList	Define suspicious post-login processes such as cmd.exe, powershell.exe, certutil.exe
AN0931	Windows	Remote Desktop (RDP) logon by a user followed by unusual process execution, file access, or lateral movement activity within a short timeframe.	WinEventLog:Security	EventCode=4624, 4648	Logon Session Creation	HostAccessPatterns	Scope detection to uncommon or first-time access between source and destination hosts
AN0931	Windows	Remote Desktop (RDP) logon by a user followed by unusual process execution, file access, or lateral movement activity within a short timeframe.	WinEventLog:Security	EventCode=4778, EventCode=4779	Logon Session Metadata	TimeWindow	Temporal threshold to correlate login with post-login activity (e.g., 5 minutes)
AN0931	Windows	Remote Desktop (RDP) logon by a user followed by unusual process execution, file access, or lateral movement activity within a short timeframe.	WinEventLog:Security	EventCode=4778, EventCode=4779	Logon Session Metadata	UserContext	Tune for non-admin users or service accounts expected to use RDP
AN0931	Windows	Remote Desktop (RDP) logon by a user followed by unusual process execution, file access, or lateral movement activity within a short timeframe.	WinEventLog:Security	EventCode=4778, EventCode=4779	Logon Session Metadata	ProcessList	Define suspicious post-login processes such as cmd.exe, powershell.exe, certutil.exe
AN0931	Windows	Remote Desktop (RDP) logon by a user followed by unusual process execution, file access, or lateral movement activity within a short timeframe.	WinEventLog:Security	EventCode=4778, EventCode=4779	Logon Session Metadata	HostAccessPatterns	Scope detection to uncommon or first-time access between source and destination hosts
AN0931	Windows	Remote Desktop (RDP) logon by a user followed by unusual process execution, file access, or lateral movement activity within a short timeframe.	WinEventLog:Sysmon	EventCode=3, 22	Network Connection Creation	TimeWindow	Temporal threshold to correlate login with post-login activity (e.g., 5 minutes)

AN	Platform	Detection Statement	Data Component Elements (DC)			Mutable Elements	
			Name	Channel	Data Component	Field	Description
AN0931	Windows	Remote Desktop (RDP) logon by a user followed by unusual process execution, file access, or lateral movement activity within a short timeframe.	WinEventLog:Sysmon	EventCode=3, 22	Network Connection Creation	UserContext	Tune for non-admin users or service accounts expected to use RDP
AN0931	Windows	Remote Desktop (RDP) logon by a user followed by unusual process execution, file access, or lateral movement activity within a short timeframe.	WinEventLog:Sysmon	EventCode=3, 22	Network Connection Creation	ProcessList	Define suspicious post-login processes such as cmd.exe, powershell.exe, certutil.exe
AN0931	Windows	Remote Desktop (RDP) logon by a user followed by unusual process execution, file access, or lateral movement activity within a short timeframe.	WinEventLog:Sysmon	EventCode=3, 22	Network Connection Creation	HostAccessPatterns	Scope detection to uncommon or first-time access between source and destination hosts
AN0931	Windows	Remote Desktop (RDP) logon by a user followed by unusual process execution, file access, or lateral movement activity within a short timeframe.	WinEventLog:Sysmon	EventCode=1	Process Creation	TimeWindow	Temporal threshold to correlate login with post-login activity (e.g., 5 minutes)
AN0931	Windows	Remote Desktop (RDP) logon by a user followed by unusual process execution, file access, or lateral movement activity within a short timeframe.	WinEventLog:Sysmon	EventCode=1	Process Creation	UserContext	Tune for non-admin users or service accounts expected to use RDP
AN0931	Windows	Remote Desktop (RDP) logon by a user followed by unusual process execution, file access, or lateral movement activity within a short timeframe.	WinEventLog:Sysmon	EventCode=1	Process Creation	ProcessList	Define suspicious post-login processes such as cmd.exe, powershell.exe, certutil.exe
AN0931	Windows	Remote Desktop (RDP) logon by a user followed by unusual process execution, file access, or lateral movement activity within a short timeframe.	WinEventLog:Sysmon	EventCode=1	Process Creation	HostAccessPatterns	Scope detection to uncommon or first-time access between source and destination hosts

Detection Strategies

Detection Strategy ID (DET0530)

Detection Strategy Name (Multi-Event Detection for SMB Admin Share Lateral Movement)

Analytic (AN1468 to AN1468)

Analytic Elements

AN	Platform	Detection Statement	Data Component Elements (DC)			Mutable Elements	
			Name	Channel	Data Component	Field	Description
AN1468	Windows	An SMB-based remote file share access followed by lateral movement actions such as remote service creation, task scheduling, or suspicious process execution on the target host using ADMIN$ or C$ shares.	WinEventLog:Security	EventCode=4624, 4648	Logon Session Creation	ShareName	Targeted admin share path, such as C$, ADMIN$, IPC$
AN1468	Windows	An SMB-based remote file share access followed by lateral movement actions such as remote service creation, task scheduling, or suspicious process execution on the target host using ADMIN$ or C$ shares.	WinEventLog:Security	EventCode=4624, 4648	Logon Session Creation	TimeWindow	Correlation window between remote file access and remote execution (e.g., 5-10 minutes)
AN1468	Windows	An SMB-based remote file share access followed by lateral movement actions such as remote service creation, task scheduling, or suspicious process execution on the target host using ADMIN$ or C$ shares.	WinEventLog:Security	EventCode=4624, 4648	Logon Session Creation	UserContext	Distinguish expected remote administrators vs. rare/first-time access by specific users
AN1468	Windows	An SMB-based remote file share access followed by lateral movement actions such as remote service creation, task scheduling, or suspicious process execution on the target host using ADMIN$ or C$ shares.	WinEventLog:Security	EventCode=4624, 4648	Logon Session Creation	ProcessList	List of suspicious binaries or tools executed post remote copy (e.g., cmd.exe, powershell.exe, runonce.exe)
AN1468	Windows	An SMB-based remote file share access followed by lateral movement actions such as remote service creation, task scheduling, or suspicious process execution on the target host using ADMIN$ or C$ shares.	WinEventLog:Sysmon	EventCode=3, 22	Network Connection Creation	ShareName	Targeted admin share path, such as C$, ADMIN$, IPC$
AN1468	Windows	An SMB-based remote file share access followed by lateral movement actions such as remote service creation, task scheduling, or suspicious process execution on the target host using ADMIN$ or C$ shares.	WinEventLog:Sysmon	EventCode=3, 22	Network Connection Creation	TimeWindow	Correlation window between remote file access and remote execution (e.g., 5-10 minutes)
AN1468	Windows	An SMB-based remote file share access followed by lateral movement actions such as remote service creation, task scheduling, or suspicious process execution on the target host using ADMIN$ or C$ shares.	WinEventLog:Sysmon	EventCode=3, 22	Network Connection Creation	UserContext	Distinguish expected remote administrators vs. rare/first-time access by specific users

AN	Platform	Detection Statement	Data Component Elements (DC)			Mutable Elements	
			Name	Channel	Data Component	Field	Description
AN1468	Windows	An SMB-based remote file share access followed by lateral movement actions such as remote service creation, task scheduling, or suspicious process execution on the target host using ADMIN$ or C$ shares.	WinEventLog:Sysmon	EventCode=3, 22	Network Connection Creation	ProcessList	List of suspicious binaries or tools executed post remote copy (e.g., cmd.exe, powershell.exe, runonce.exe)
AN1468	Windows	An SMB-based remote file share access followed by lateral movement actions such as remote service creation, task scheduling, or suspicious process execution on the target host using ADMIN$ or C$ shares.	WinEventLog:Sysmon	EventCode=1	Process Creation	ShareName	Targeted admin share path, such as C$, ADMIN$, IPC$
AN1468	Windows	An SMB-based remote file share access followed by lateral movement actions such as remote service creation, task scheduling, or suspicious process execution on the target host using ADMIN$ or C$ shares.	WinEventLog:Sysmon	EventCode=1	Process Creation	TimeWindow	Correlation window between remote file access and remote execution (e.g., 5-10 minutes)
AN1468	Windows	An SMB-based remote file share access followed by lateral movement actions such as remote service creation, task scheduling, or suspicious process execution on the target host using ADMIN$ or C$ shares.	WinEventLog:Sysmon	EventCode=1	Process Creation	UserContext	Distinguish expected remote administrators vs. rare/first-time access by specific users
AN1468	Windows	An SMB-based remote file share access followed by lateral movement actions such as remote service creation, task scheduling, or suspicious process execution on the target host using ADMIN$ or C$ shares.	WinEventLog:Sysmon	EventCode=1	Process Creation	ProcessList	List of suspicious binaries or tools executed post remote copy (e.g., cmd.exe, powershell.exe, runonce.exe)

Detection Strategies

Detection Strategy ID (DET0347)

Detection Strategy Name (Detection Strategy for Masquerading via Legitimate Resource Name or Location)

Analytic (AN0983 to AN0983)

Analytic Elements

AN	Platform	Detection Statement	Data Component Elements (DC)			Mutable Elements	
			Name	Channel	Data Component	Field	Description
AN0983	Windows	Detects processes or binaries executed from trusted directories (e.g., System32) or using trusted names (e.g., svchost.exe) where the metadata, hash, or parent process does not align with legitimate activity patterns.	WinEventLog:Security	EventCode=4688	Process Creation	trusted_directory_list	Paths such as C:\Windows\System32 that adversaries may abuse
AN0983	Windows	Detects processes or binaries executed from trusted directories (e.g., System32) or using trusted names (e.g., svchost.exe) where the metadata, hash, or parent process does not align with legitimate activity patterns.	WinEventLog:Security	EventCode=4688	Process Creation	process_baseline_age	Time window to determine process novelty (e.g., 30 days)
AN0983	Windows	Detects processes or binaries executed from trusted directories (e.g., System32) or using trusted names (e.g., svchost.exe) where the metadata, hash, or parent process does not align with legitimate activity patterns.	WinEventLog:Sysmon	EventCode=11	File Creation	trusted_directory_list	Paths such as C:\Windows\System32 that adversaries may abuse
AN0983	Windows	Detects processes or binaries executed from trusted directories (e.g., System32) or using trusted names (e.g., svchost.exe) where the metadata, hash, or parent process does not align with legitimate activity patterns.	WinEventLog:Sysmon	EventCode=11	File Creation	process_baseline_age	Time window to determine process novelty (e.g., 30 days)

Detection Strategies

Detection Strategy ID (DET0441)

Detection Strategy Name (Detection of Suspicious Scheduled Task Creation and Execution on Windows)

Analytic (AN1221 to AN1221)

Analytic Elements

AN	Platform	Detection Statement	Data Component Elements (DC)			Mutable Elements	
			Name	Channel	Data Component	Field	Description
AN1221	Windows	Detects the creation, modification, or deletion of scheduled tasks through Task Scheduler, WMI, PowerShell, or API-based methods followed by execution from svchost.exe or taskeng.exe. Includes detection of hidden or anomalous scheduled tasks, especially those created under SYSTEM or suspicious user contexts.	WinEventLog:Security	EventCode=4698	Scheduled Job Creation	TimeWindow	Defines threshold for grouping task creation and associated execution within suspicious time proximity.
AN1221	Windows	Detects the creation, modification, or deletion of scheduled tasks through Task Scheduler, WMI, PowerShell, or API-based methods followed by execution from svchost.exe or taskeng.exe. Includes detection of hidden or anomalous scheduled tasks, especially those created under SYSTEM or suspicious user contexts.	WinEventLog:Security	EventCode=4698	Scheduled Job Creation	UserContext	Filters based on non-standard user accounts or execution under SYSTEM when not typical for the environment.
AN1221	Windows	Detects the creation, modification, or deletion of scheduled tasks through Task Scheduler, WMI, PowerShell, or API-based methods followed by execution from svchost.exe or taskeng.exe. Includes detection of hidden or anomalous scheduled tasks, especially those created under SYSTEM or suspicious user contexts.	WinEventLog:Security	EventCode=4698	Scheduled Job Creation	TaskNamePattern	Allows defenders to flag obfuscated, randomized, or suspicious task names outside normal conventions.
AN1221	Windows	Detects the creation, modification, or deletion of scheduled tasks through Task Scheduler, WMI, PowerShell, or API-based methods followed by execution from svchost.exe or taskeng.exe. Includes detection of hidden or anomalous scheduled tasks, especially those created under SYSTEM or suspicious user contexts.	WinEventLog:Security	EventCode=4698	Scheduled Job Creation	CommandLineEntropy Threshold	Flags tasks executing heavily obfuscated PowerShell or binary blobs via base64 or encoding.
AN1221	Windows	Detects the creation, modification, or deletion of scheduled tasks through Task Scheduler, WMI, PowerShell, or API-based methods followed by execution from svchost.exe or taskeng.exe. Includes detection of hidden or anomalous scheduled tasks, especially those created under SYSTEM or suspicious user contexts.	WinEventLog:Security	EventCode=4702	Scheduled Job Modification	TimeWindow	Defines threshold for grouping task creation and associated execution within suspicious time proximity.

AN	Platform	Detection Statement	Data Component Elements (DC)			Mutable Elements	
			Name	Channel	Data Component	Field	Description
AN1221	Windows	Detects the creation, modification, or deletion of scheduled tasks through Task Scheduler, WMI, PowerShell, or API-based methods followed by execution from svchost.exe or taskeng.exe. Includes detection of hidden or anomalous scheduled tasks, especially those created under SYSTEM or suspicious user contexts.	WinEventLog:Security	EventCode=4702	Scheduled Job Modification	UserContext	Filters based on non-standard user accounts or execution under SYSTEM when not typical for the environment.
AN1221	Windows	Detects the creation, modification, or deletion of scheduled tasks through Task Scheduler, WMI, PowerShell, or API-based methods followed by execution from svchost.exe or taskeng.exe. Includes detection of hidden or anomalous scheduled tasks, especially those created under SYSTEM or suspicious user contexts.	WinEventLog:Security	EventCode=4702	Scheduled Job Modification	TaskNamePattern	Allows defenders to flag obfuscated, randomized, or suspicious task names outside normal conventions.
AN1221	Windows	Detects the creation, modification, or deletion of scheduled tasks through Task Scheduler, WMI, PowerShell, or API-based methods followed by execution from svchost.exe or taskeng.exe. Includes detection of hidden or anomalous scheduled tasks, especially those created under SYSTEM or suspicious user contexts.	WinEventLog:Security	EventCode=4702	Scheduled Job Modification	CommandLineEntropy Threshold	Flags tasks executing heavily obfuscated PowerShell or binary blobs via base64 or encoding.
AN1221	Windows	Detects the creation, modification, or deletion of scheduled tasks through Task Scheduler, WMI, PowerShell, or API-based methods followed by execution from svchost.exe or taskeng.exe. Includes detection of hidden or anomalous scheduled tasks, especially those created under SYSTEM or suspicious user contexts.	WinEventLog:Sysmon	EventCode=1	Process Creation	TimeWindow	Defines threshold for grouping task creation and associated execution within suspicious time proximity.
AN1221	Windows	Detects the creation, modification, or deletion of scheduled tasks through Task Scheduler, WMI, PowerShell, or API-based methods followed by execution from svchost.exe or taskeng.exe. Includes detection of hidden or anomalous scheduled tasks, especially those created under SYSTEM or suspicious user contexts.	WinEventLog:Sysmon	EventCode=1	Process Creation	UserContext	Filters based on non-standard user accounts or execution under SYSTEM when not typical for the environment.
AN	Platform	Detection Statement	Data Component Elements (DC)			Mutable Elements	
			Name	Channel	Data Component	Field	Description
AN1221	Windows	Detects the creation, modification, or deletion of scheduled tasks through Task Scheduler, WMI, PowerShell, or API-based methods followed by	WinEventLog:Sysmon	EventCode=1	Process Creation	TaskNamePattern	Allows defenders to flag obfuscated, randomized, or suspicious task names

AN	Platform	Detection Statement	Data Component Elements (DC)			Mutable Elements	
			Name	Channel	Data Component	Field	Description
		execution from svchost.exe or taskeng.exe. Includes detection of hidden or anomalous scheduled tasks, especially those created under SYSTEM or suspicious user contexts.					outside normal conventions.
AN1221	Windows	Detects the creation, modification, or deletion of scheduled tasks through Task Scheduler, WMI, PowerShell, or API-based methods followed by execution from svchost.exe or taskeng.exe. Includes detection of hidden or anomalous scheduled tasks, especially those created under SYSTEM or suspicious user contexts.	WinEventLog:Sysmon	EventCode=1	Process Creation	CommandLineEntropyThreshold	Flags tasks executing heavily obfuscated PowerShell or binary blobs via base64 or encoding.
AN1221	Windows	Detects the creation, modification, or deletion of scheduled tasks through Task Scheduler, WMI, PowerShell, or API-based methods followed by execution from svchost.exe or taskeng.exe. Includes detection of hidden or anomalous scheduled tasks, especially those created under SYSTEM or suspicious user contexts.	WinEventLog:Sysmon	EventCode=11	File Creation	TimeWindow	Defines threshold for grouping task creation and associated execution within suspicious time proximity.
AN1221	Windows	Detects the creation, modification, or deletion of scheduled tasks through Task Scheduler, WMI, PowerShell, or API-based methods followed by execution from svchost.exe or taskeng.exe. Includes detection of hidden or anomalous scheduled tasks, especially those created under SYSTEM or suspicious user contexts.	WinEventLog:Sysmon	EventCode=11	File Creation	UserContext	Filters based on non-standard user accounts or execution under SYSTEM when not typical for the environment.
AN1221	Windows	Detects the creation, modification, or deletion of scheduled tasks through Task Scheduler, WMI, PowerShell, or API-based methods followed by execution from svchost.exe or taskeng.exe. Includes detection of hidden or anomalous scheduled tasks, especially those created under SYSTEM or suspicious user contexts.	WinEventLog:Sysmon	EventCode=11	File Creation	TaskNamePattern	Allows defenders to flag obfuscated, randomized, or suspicious task names outside normal conventions.
AN1221	Windows	Detects the creation, modification, or deletion of scheduled tasks through Task Scheduler, WMI, PowerShell, or API-based methods followed by execution from svchost.exe or taskeng.exe. Includes detection of hidden or anomalous scheduled tasks, especially those created under SYSTEM or suspicious user contexts.	WinEventLog:Sysmon	EventCode=11	File Creation	CommandLineEntropyThreshold	Flags tasks executing heavily obfuscated PowerShell or binary blobs via base64 or encoding.

AN	Platform	Detection Statement	Data Component Elements (DC)			Mutable Elements	
			Name	Channel	Data Component	Field	Description
AN1221	Windows	Detects the creation, modification, or deletion of scheduled tasks through Task Scheduler, WMI, PowerShell, or API-based methods followed by execution from svchost.exe or taskeng.exe. Includes detection of hidden or anomalous scheduled tasks, especially those created under SYSTEM or suspicious user contexts.	WinEventLog:Sysmon	EventCode=13, 14	Windows Registry Key Modification	TimeWindow	Defines threshold for grouping task creation and associated execution within suspicious time proximity.
AN1221	Windows	Detects the creation, modification, or deletion of scheduled tasks through Task Scheduler, WMI, PowerShell, or API-based methods followed by execution from svchost.exe or taskeng.exe. Includes detection of hidden or anomalous scheduled tasks, especially those created under SYSTEM or suspicious user contexts.	WinEventLog:Sysmon	EventCode=13, 14	Windows Registry Key Modification	UserContext	Filters based on non-standard user accounts or execution under SYSTEM when not typical for the environment.
AN1221	Windows	Detects the creation, modification, or deletion of scheduled tasks through Task Scheduler, WMI, PowerShell, or API-based methods followed by execution from svchost.exe or taskeng.exe. Includes detection of hidden or anomalous scheduled tasks, especially those created under SYSTEM or suspicious user contexts.	WinEventLog:Sysmon	EventCode=13, 14	Windows Registry Key Modification	TaskNamePattern	Allows defenders to flag obfuscated, randomized, or suspicious task names outside normal conventions.
AN1221	Windows	Detects the creation, modification, or deletion of scheduled tasks through Task Scheduler, WMI, PowerShell, or API-based methods followed by execution from svchost.exe or taskeng.exe. Includes detection of hidden or anomalous scheduled tasks, especially those created under SYSTEM or suspicious user contexts.	WinEventLog:Sysmon	EventCode=13, 14	Windows Registry Key Modification	CommandLineEntropy Threshold	Flags tasks executing heavily obfuscated PowerShell or binary blobs via base64 or encoding.

Detection Strategies

Detection Strategy ID (DET0389)

Detection Strategy Name (Behavioral Detection of DLL Injection via Windows API)

Analytic (AN1095 to AN1095)

Analytic Elements

AN	Platform	Detection Statement	Data Component Elements (DC)			Mutable Elements	
			Name	Channel	Data Component	Field	Description
AN1095	Windows	Detects DLL injection through correlation of memory allocation and writing to remote process memory (e.g., VirtualAllocEx, WriteProcessMemory), followed by remote thread creation (e.g., CreateRemoteThread) that loads a suspicious or unsigned DLL using LoadLibrary or reflective loading.	WinEventLog:Sysmon	EventCode=10	Process Access	InjectedDLLSignatureStatus	Whether the DLL is unsigned, untrusted, or loaded from a non-standard path
AN1095	Windows	Detects DLL injection through correlation of memory allocation and writing to remote process memory (e.g., VirtualAllocEx, WriteProcessMemory), followed by remote thread creation (e.g., CreateRemoteThread) that loads a suspicious or unsigned DLL using LoadLibrary or reflective loading.	WinEventLog:Sysmon	EventCode=10	Process Access	TimeWindow	Temporal correlation threshold between memory operations and thread creation
AN1095	Windows	Detects DLL injection through correlation of memory allocation and writing to remote process memory (e.g., VirtualAllocEx, WriteProcessMemory), followed by remote thread creation (e.g., CreateRemoteThread) that loads a suspicious or unsigned DLL using LoadLibrary or reflective loading.	WinEventLog:Sysmon	EventCode=10	Process Access	TargetProcessList	List of sensitive or high-value processes targeted for injection (e.g., explorer.exe, winlogon.exe)
AN1095	Windows	Detects DLL injection through correlation of memory allocation and writing to remote process memory (e.g., VirtualAllocEx, WriteProcessMemory), followed by remote thread creation (e.g., CreateRemoteThread) that loads a suspicious or unsigned DLL using LoadLibrary or reflective loading.	WinEventLog:Sysmon	EventCode=10	Process Access	ParentProcessAnomalyThreshold	Degree of deviation from expected parent-child lineage
AN1095	Windows	Detects DLL injection through correlation of memory allocation and writing to remote process memory (e.g., VirtualAllocEx, WriteProcessMemory), followed by remote thread creation (e.g., CreateRemoteThread) that loads a suspicious or unsigned DLL using LoadLibrary or reflective loading.	WinEventLog:Sysmon	EventCode=1	Process Creation	InjectedDLLSignatureStatus	Whether the DLL is unsigned, untrusted, or loaded from a non-standard path

AN	Platform	Detection Statement	Data Component Elements (DC)			Mutable Elements	
			Name	Channel	Data Component	Field	Description
AN1095	Windows	Detects DLL injection through correlation of memory allocation and	WinEventLog:Sysmon	EventCode=1	Process Creation	TimeWindow	Temporal correlation threshold between memory

AN	Platform	Detection Statement	Data Component Elements (DC)			Mutable Elements	
			Name	Channel	Data Component	Field	Description
		writing to remote process memory (e.g., VirtualAllocEx, WriteProcessMemory), followed by remote thread creation (e.g., CreateRemoteThread) that loads a suspicious or unsigned DLL using LoadLibrary or reflective loading.					operations and threadcreation
AN1095	Windows	Detects DLL injection through correlation of memory allocation and writing to remote process memory (e.g., VirtualAllocEx, WriteProcessMemory), followed by remote thread creation (e.g., CreateRemoteThread) that loads a suspicious or unsigned DLL using LoadLibrary or reflective loading.	WinEventLog:Sysmon	EventCode=1	Process Creation	TargetProcessList	List of sensitive or high-value processes targeted for injection (e.g., explorer.exe, winlogon.exe)
AN1095	Windows	Detects DLL injection through correlation of memory allocation and writing to remote process memory (e.g., VirtualAllocEx, WriteProcessMemory), followed by remote thread creation (e.g., CreateRemoteThread) that loads a suspicious or unsigned DLL using LoadLibrary or reflective loading.	WinEventLog:Sysmon	EventCode=1	Process Creation	ParentProcessAnomalyThreshold	Degree of deviation from expected parent-child lineage
AN1095	Windows	Detects DLL injection through correlation of memory allocation and writing to remote process memory (e.g., VirtualAllocEx, WriteProcessMemory), followed by remote thread creation (e.g., CreateRemoteThread) that loads a suspicious or unsigned DLL using LoadLibrary or reflective loading.	WinEventLog:Sysmon	EventCode=7	Module Load	InjectedDLLSignatureStatus	Whether the DLL is unsigned, untrusted, or loaded from a non-standard path
AN1095	Windows	Detects DLL injection through correlation of memory allocation and writing to remote process memory (e.g., VirtualAllocEx, WriteProcessMemory), followed by remote thread creation (e.g., CreateRemoteThread) that loads a suspicious or unsigned DLL using LoadLibrary or reflective loading.	WinEventLog:Sysmon	EventCode=7	Module Load	TimeWindow	Temporal correlation threshold between memory operations and thread creation
AN1095	Windows	Detects DLL injection through correlation of memory allocation and writing to remote process memory (e.g., VirtualAllocEx, WriteProcessMemory), followed by remote thread creation (e.g., CreateRemoteThread) that loads a suspicious or unsigned DLL using LoadLibrary or reflective loading.	WinEventLog:Sysmon	EventCode=7	Module Load	TargetProcessList	List of sensitive or high-value processes targeted for injection (e.g., explorer.exe, winlogon.exe)

AN	Platform	Detection Statement	Data Component Elements (DC)			Mutable Elements	
			Name	Channel	Data Component	Field	Description
AN1095	Windows	Detects DLL injection through correlation of memory allocation and	WinEventLog:Sysmon	EventCode=7	Module Load	ParentProcessAnomalyThreshold	Degree of deviation from expected parent-child

AN	Platform	Detection Statement	Data Component Elements (DC)			Mutable Elements	
			Name	Channel	Data Component	Field	Description
		writing to remote process memory (e.g., VirtualAllocEx, WriteProcessMemory), followed by remote thread creation (e.g., CreateRemoteThread) that loads a suspicious or unsigned DLL using LoadLibrary or reflective loading.					lineage
AN1095	Windows	Detects DLL injection through correlation of memory allocation and writing to remote process memory (e.g., VirtualAllocEx, WriteProcessMemory), followed by remote thread creation (e.g., CreateRemoteThread) that loads a suspicious or unsigned DLL using LoadLibrary or reflective loading.	WinEventLog:Sysmon	EventCode=17	Named Pipe Metadata	InjectedDLLSignatureStatus	Whether the DLL is unsigned, untrusted, or loaded from a non-standard path
AN1095	Windows	Detects DLL injection through correlation of memory allocation and writing to remote process memory (e.g., VirtualAllocEx, WriteProcessMemory), followed by remote thread creation (e.g., CreateRemoteThread) that loads a suspicious or unsigned DLL using LoadLibrary or reflective loading.	WinEventLog:Sysmon	EventCode=17	Named Pipe Metadata	TimeWindow	Temporal correlation threshold between memory operations and thread creation
AN1095	Windows	Detects DLL injection through correlation of memory allocation and writing to remote process memory (e.g., VirtualAllocEx, WriteProcessMemory), followed by remote thread creation (e.g., CreateRemoteThread) that loads a suspicious or unsigned DLL using LoadLibrary or reflective loading.	WinEventLog:Sysmon	EventCode=17	Named Pipe Metadata	TargetProcessList	List of sensitive or high-value processes targeted for injection (e.g., explorer.exe, winlogon.exe)
AN1095	Windows	Detects DLL injection through correlation of memory allocation and writing to remote process memory (e.g., VirtualAllocEx, WriteProcessMemory), followed by remote thread creation (e.g., CreateRemoteThread) that loads a suspicious or unsigned DLL using LoadLibrary or reflective loading.	WinEventLog:Sysmon	EventCode=17	Named Pipe Metadata	ParentProcessAnomalyThreshold	Degree of deviation from expected parent-child lineage

Detection Strategies

Detection Strategy ID (DET0455)

Detection Strategy Name (Abuse of PowerShell for Arbitrary Execution)

Analytic (AN1252 to AN1252)

Analytic Elements

AN	Platform	Detection Statement	Data Component Elements (DC)			Mutable Elements	
			Name	Channel	Data Component	Field	Description
AN1252	Windows	Detects behavioral chains where PowerShell is launched with encoded commands, unusual parent processes, or suspicious modules loaded, potentially followed by network connections or child process spawning. Supports detection of both direct (powershell.exe) and indirect (.NET automation) invocations.	WinEventLog:Sysmon	EventCode=1	Process Creation	CommandLinePattern	Regex pattern for encoded, obfuscated, or hidden PowerShell arguments (e.g., '-enc', '-nop').
AN1252	Windows	Detects behavioral chains where PowerShell is launched with encoded commands, unusual parent processes, or suspicious modules loaded, potentially followed by network connections or child process spawning. Supports detection of both direct (powershell.exe) and indirect (.NET automation) invocations.	WinEventLog:Sysmon	EventCode=1	Process Creation	ParentProcessName	Filter based on abnormal parents like Excel, WinWord, or mshta spawning PowerShell.
AN1252	Windows	Detects behavioral chains where PowerShell is launched with encoded commands, unusual parent processes, or suspicious modules loaded, potentially followed by network connections or child process spawning. Supports detection of both direct (powershell.exe) and indirect (.NET automation) invocations.	WinEventLog:Sysmon	EventCode=1	Process Creation	TimeWindow	Scope detection to off-hours, lateral movement timeframes, or non-maintenance windows.
AN1252	Windows	Detects behavioral chains where PowerShell is launched with encoded commands, unusual parent processes, or suspicious modules loaded, potentially followed by network connections or child process spawning. Supports detection of both direct (powershell.exe) and indirect (.NET automation) invocations.	WinEventLog:Sysmon	EventCode=1	Process Creation	LoadedModuleList	Tuneable to monitor rare or never-before-seen .NET assemblies tied to PowerShell abuse.
AN1252	Windows	Detects behavioral chains where PowerShell is launched with encoded commands, unusual parent processes, or suspicious modules loaded, potentially followed by network connections or child process spawning. Supports detection of both direct (powershell.exe) and indirect (.NET automation) invocations.	WinEventLog:Sysmon	EventCode=1	Process Creation	ScriptBlockLengthThreshold	Adjustable threshold for length of script blocks logged by Event ID 4104 (useful for filtering noise).

AN	Platform	Detection Statement	Data Component Elements (DC)			Mutable Elements	
			Name	Channel	Data Component	Field	Description
AN1252	Windows	Detects behavioral chains where PowerShell is launched with encoded commands, unusual parent processes, or suspicious modules loaded, potentially followed by network connections or child process spawning. Supports detection of both direct (powershell.exe) and indirect (.NET automation) invocations.	WinEventLog:PowerShell	EventCode=4103, 4104, 4105, 4106	Command Execution	CommandLinePattern	Regex pattern for encoded, obfuscated, or hidden PowerShell arguments (e.g., '-enc', '-nop').
AN1252	Windows	Detects behavioral chains where PowerShell is launched with encoded commands, unusual parent processes, or suspicious modules loaded, potentially followed by network connections or child process spawning. Supports detection of both direct (powershell.exe) and indirect (.NET automation) invocations.	WinEventLog:PowerShell	EventCode=4103, 4104, 4105, 4106	Command Execution	ParentProcessName	Filter based on abnormal parents like Excel, WinWord, or mshta spawning PowerShell.
AN1252	Windows	Detects behavioral chains where PowerShell is launched with encoded commands, unusual parent processes, or suspicious modules loaded, potentially followed by network connections or child process spawning. Supports detection of both direct (powershell.exe) and indirect (.NET automation) invocations.	WinEventLog:PowerShell	EventCode=4103, 4104, 4105, 4106	Command Execution	TimeWindow	Scope detection to off-hours, lateral movement timeframes, or non-maintenance windows.
AN1252	Windows	Detects behavioral chains where PowerShell is launched with encoded commands, unusual parent processes, or suspicious modules loaded, potentially followed by network connections or child process spawning. Supports detection of both direct (powershell.exe) and indirect (.NET automation) invocations.	WinEventLog:PowerShell	EventCode=4103, 4104, 4105, 4106	Command Execution	LoadedModuleList	Tuneable to monitor rare or never-before-seen .NET assemblies tied to PowerShell abuse.
AN1252	Windows	Detects behavioral chains where PowerShell is launched with encoded commands, unusual parent processes, or suspicious modules loaded, potentially followed by network connections or child process spawning. Supports detection of both direct (powershell.exe) and indirect (.NET automation) invocations.	WinEventLog:PowerShell	EventCode=4103, 4104, 4105, 4106	Command Execution	ScriptBlockLengthThreshold	Adjustable threshold for length of script blocks logged by Event ID 4104 (useful for filtering noise).

AN	Platform	Detection Statement	Data Component Elements (DC)			Mutable Elements	
			Name	Channel	Data Component	Field	Description
AN1252	Windows	Detects behavioral chains where PowerShell is launched with encoded commands, unusual parent processes, or suspicious modules loaded,	WinEventLog:PowerShell	EventCode=400, 403	Process Metadata	CommandLinePattern	Regex pattern for encoded, obfuscated, or hidden PowerShell arguments

AN	Platform	Detection Statement	Data Component Elements (DC)			Mutable Elements	
			Name	Channel	Data Component	Field	Description
		potentially followed by network connections or child process spawning. Supports detection of both direct (powershell.exe) and indirect (.NET automation) invocations.					(e.g., '-enc', '-nop').
AN1252	Windows	Detects behavioral chains where PowerShell is launched with encoded commands, unusual parent processes, or suspicious modules loaded, potentially followed by network connections or child process spawning. Supports detection of both direct (powershell.exe) and indirect (.NET automation) invocations.	WinEventLog:PowerShell	EventCode=400, 403	Process Metadata	ParentProcessName	Filter based on abnormal parents like Excel, WinWord, or mshta spawning PowerShell.
AN1252	Windows	Detects behavioral chains where PowerShell is launched with encoded commands, unusual parent processes, or suspicious modules loaded, potentially followed by network connections or child process spawning. Supports detection of both direct (powershell.exe) and indirect (.NET automation) invocations.	WinEventLog:PowerShell	EventCode=400, 403	Process Metadata	TimeWindow	Scope detection to off-hours, lateral movement timeframes, or non-maintenance windows.
AN1252	Windows	Detects behavioral chains where PowerShell is launched with encoded commands, unusual parent processes, or suspicious modules loaded, potentially followed by network connections or child process spawning. Supports detection of both direct (powershell.exe) and indirect (.NET automation) invocations.	WinEventLog:PowerShell	EventCode=400, 403	Process Metadata	LoadedModuleList	Tuneable to monitor rare or never-before-seen .NET assemblies tied to PowerShell abuse.
AN1252	Windows	Detects behavioral chains where PowerShell is launched with encoded commands, unusual parent processes, or suspicious modules loaded, potentially followed by network connections or child process spawning. Supports detection of both direct (powershell.exe) and indirect (.NET automation) invocations.	WinEventLog:PowerShell	EventCode=400, 403	Process Metadata	ScriptBlockLengthThreshold	Adjustable threshold for length of script blocks logged by Event ID 4104 (useful for filtering noise).
AN1252	Windows	Detects behavioral chains where PowerShell is launched with encoded commands, unusual parent processes, or suspicious modules loaded, potentially followed by network connections or child process spawning. Supports detection of both direct (powershell.exe) and indirect (.NET automation) invocations.	WinEventLog:Sysmon	EventCode=7	Module Load	CommandLinePattern	Regex pattern for encoded, obfuscated, or hidden PowerShell arguments (e.g., '-enc', '-nop').

AN	Platform	Detection Statement	Data Component Elements (DC)			Mutable Elements	
			Name	Channel	Data Component	Field	Description
AN1252	Windows	Detects behavioral chains where PowerShell is launched with encoded commands, unusual parent processes, or suspicious modules loaded, potentially followed by network connections or child process spawning. Supports detection of both direct (powershell.exe) and indirect (.NET automation) invocations.	WinEventLog:Sysmon	EventCode=7	Module Load	ParentProcessName	Filter based on abnormal parents like Excel, WinWord, or mshta spawning PowerShell.
AN1252	Windows	Detects behavioral chains where PowerShell is launched with encoded commands, unusual parent processes, or suspicious modules loaded, potentially followed by network connections or child process spawning. Supports detection of both direct (powershell.exe) and indirect (.NET automation) invocations.	WinEventLog:Sysmon	EventCode=7	Module Load	TimeWindow	Scope detection to off-hours, lateral movement timeframes, or non-maintenance windows.
AN1252	Windows	Detects behavioral chains where PowerShell is launched with encoded commands, unusual parent processes, or suspicious modules loaded, potentially followed by network connections or child process spawning. Supports detection of both direct (powershell.exe) and indirect (.NET automation) invocations.	WinEventLog:Sysmon	EventCode=7	Module Load	LoadedModuleList	Tuneable to monitor rare or never-before-seen .NET assemblies tied to PowerShell abuse.
AN1252	Windows	Detects behavioral chains where PowerShell is launched with encoded commands, unusual parent processes, or suspicious modules loaded, potentially followed by network connections or child process spawning. Supports detection of both direct (powershell.exe) and indirect (.NET automation) invocations.	WinEventLog:Sysmon	EventCode=7	Module Load	ScriptBlockLengthThreshold	Adjustable threshold for length of script blocks logged by Event ID 4104 (useful for filtering noise).

Detection Strategies

Detection Strategy ID (DET0140)

Detection Strategy Name (Behavioral Detection of Malicious File Deletion)

Analytic (AN0392 to AN0392)

Analytic Elements

AN	Platform	Detection Statement	Data Component Elements (DC)			Mutable Elements	
			Name	Channel	Data Component	Field	Description
AN0392	Windows	Detects adversary behavior deleting artifacts (e.g., dropped payloads, evidence files) using native or external utilities (e.g., del, erase, SDelete). Detects deletion events correlated with unusual process lineage or timing post-execution.	WinEventLog:Sysmon	EventCode=23	File Deletion	TimeWindow	Defines correlation window after suspicious binary execution or login session.
AN0392	Windows	Detects adversary behavior deleting artifacts (e.g., dropped payloads, evidence files) using native or external utilities (e.g., del, erase, SDelete). Detects deletion events correlated with unusual process lineage or timing post-execution.	WinEventLog:Sysmon	EventCode=23	File Deletion	FilePathPattern	Focuses on deletion of temp files, malware staging dirs, or known indicators.
AN0392	Windows	Detects adversary behavior deleting artifacts (e.g., dropped payloads, evidence files) using native or external utilities (e.g., del, erase, SDelete). Detects deletion events correlated with unusual process lineage or timing post-execution.	WinEventLog:Sysmon	EventCode=23	File Deletion	UserContext	Privilege level or impersonated user deleting sensitive files.
AN0392	Windows	Detects adversary behavior deleting artifacts (e.g., dropped payloads, evidence files) using native or external utilities (e.g., del, erase, SDelete). Detects deletion events correlated with unusual process lineage or timing post-execution.	WinEventLog:Security	EventCode=4663, 4670, 4656	File Access	TimeWindow	Defines correlation window after suspicious binary execution or login session.
AN0392	Windows	Detects adversary behavior deleting artifacts (e.g., dropped payloads, evidence files) using native or external utilities (e.g., del, erase, SDelete). Detects deletion events correlated with unusual process lineage or timing post-execution.	WinEventLog:Security	EventCode=4663, 4670, 4656	File Access	FilePathPattern	Focuses on deletion of temp files, malware staging dirs, or known indicators.
AN0392	Windows	Detects adversary behavior deleting artifacts (e.g., dropped payloads, evidence files) using native or external utilities (e.g., del, erase, SDelete). Detects deletion events correlated with unusual process lineage or timing post-execution.	WinEventLog:Security	EventCode=4663, 4670, 4656	File Access	UserContext	Privilege level or impersonated user deleting sensitive files.

AN	Platform	Detection Statement	Data Component Elements (DC)			Mutable Elements	
			Name	Channel	Data Component	Field	Description
AN0392	Windows	Detects adversary behavior deleting artifacts (e.g., dropped payloads, evidence files) using native or external utilities (e.g., del, erase, SDelete). Detects deletion events correlated with unusual process lineage or timing post-execution.	WinEventLog:PowerShell	EventCode=4103, 4104, 4105, 4106	Command Execution	TimeWindow	Defines correlation window after suspicious binary execution or login session.
AN0392	Windows	Detects adversary behavior deleting artifacts (e.g., dropped payloads, evidence files) using native or external utilities (e.g., del, erase, SDelete). Detects deletion events correlated with unusual process lineage or timing post-execution.	WinEventLog:PowerShell	EventCode=4103, 4104, 4105, 4106	Command Execution	FilePathPattern	Focuses on deletion of temp files, malware staging dirs, or known indicators.
AN0392	Windows	Detects adversary behavior deleting artifacts (e.g., dropped payloads, evidence files) using native or external utilities (e.g., del, erase, SDelete). Detects deletion events correlated with unusual process lineage or timing post-execution.	WinEventLog:PowerShell	EventCode=4103, 4104, 4105, 4106	Command Execution	UserContext	Privilege level or impersonated user deleting sensitive files.

Detection Strategies

Detection Strategy ID (DET0027)

Detection Strategy Name (Detection of Web Protocol-Based C2 Over HTTP, HTTPS, or WebSockets)

Analytic (AN0075 to AN0075)

Analytic Elements

AN	Platform	Detection Statement	Data Component Elements (DC)			Mutable Elements	
			Name	Channel	Data Component	Field	Description
AN0075	Windows	Detects unexpected or high-volume HTTP/S/WebSocket communication from suspicious processes (e.g., PowerShell, rundll32) using uncommon user agents or mimicking browser traffic to unusual domains or IPs.	NSM:Flow	http.log, ssl.log	Network Traffic Content	ProcessNameExclusions	Filter out legitimate browser/network utilities
AN0075	Windows	Detects unexpected or high-volume HTTP/S/WebSocket communication from suspicious processes (e.g., PowerShell, rundll32) using uncommon user agents or mimicking browser traffic to unusual domains or IPs.	NSM:Flow	http.log, ssl.log	Network Traffic Content	UserAgentAnomalies	Detect non-browser user-agents or spoofed headers
AN0075	Windows	Detects unexpected or high-volume HTTP/S/WebSocket communication from suspicious processes (e.g., PowerShell, rundll32) using uncommon user agents or mimicking browser traffic to unusual domains or IPs.	NSM:Flow	http.log, ssl.log	Network Traffic Content	OutboundByteRatioThreshold	Flag when outbound > inbound volume by 90%+
AN0075	Windows	Detects unexpected or high-volume HTTP/S/WebSocket communication from suspicious processes (e.g., PowerShell, rundll32) using uncommon user agents or mimicking browser traffic to unusual domains or IPs.	WinEventLog:Sysmon	EventCode=3, 22	Network Connection Creation	ProcessNameExclusions	Filter out legitimate browser/network utilities
AN0075	Windows	Detects unexpected or high-volume HTTP/S/WebSocket communication from suspicious processes (e.g., PowerShell, rundll32) using uncommon user agents or mimicking browser traffic to unusual domains or IPs.	WinEventLog:Sysmon	EventCode=3, 22	Network Connection Creation	UserAgentAnomalies	Detect non-browser user-agents or spoofed headers
AN0075	Windows	Detects unexpected or high-volume HTTP/S/WebSocket communication from suspicious processes (e.g., PowerShell, rundll32) using uncommon user agents or mimicking browser traffic to unusual domains or IPs.	WinEventLog:Sysmon	EventCode=3, 22	Network Connection Creation	OutboundByteRatioThreshold	Flag when outbound > inbound volume by 90%+

Detection Strategies

Detection Strategy ID (DET0370)

Detection Strategy Name (Recursive Enumeration of Files and Directories Across Privilege Contexts)

Analytic (AN1040 to AN1040)

Analytic Elements

AN	Platform	Detection Statement	Data Component Elements (DC)			Mutable Elements	
			Name	Channel	Data Component	Field	Description
AN1040	Windows	Execution of file enumeration commands (e.g., 'dir', 'tree') from non-standard processes or unusual user contexts, followed by recursive directory traversal or access to sensitive locations.	WinEventLog:Security	EventCode=4688	Process Creation	CommandLineRegex	Allows tuning based on tools/scripts used for enumeration (e.g., tree, dir /s /b)
AN1040	Windows	Execution of file enumeration commands (e.g., 'dir', 'tree') from non-standard processes or unusual user contexts, followed by recursive directory traversal or access to sensitive locations.	WinEventLog:Security	EventCode=4688	Process Creation	UserContext	Scoping for standard vs elevated or service accounts
AN1040	Windows	Execution of file enumeration commands (e.g., 'dir', 'tree') from non-standard processes or unusual user contexts, followed by recursive directory traversal or access to sensitive locations.	WinEventLog:Security	EventCode=4688	Process Creation	TimeWindow	Defines burst activity over short periods (e.g., >50 directory queries in 30s)
AN1040	Windows	Execution of file enumeration commands (e.g., 'dir', 'tree') from non-standard processes or unusual user contexts, followed by recursive directory traversal or access to sensitive locations.	WinEventLog:Sysmon	EventCode=11	File Creation	CommandLineRegex	Allows tuning based on tools/scripts used for enumeration (e.g., tree, dir /s /b)
AN1040	Windows	Execution of file enumeration commands (e.g., 'dir', 'tree') from non-standard processes or unusual user contexts, followed by recursive directory traversal or access to sensitive locations.	WinEventLog:Sysmon	EventCode=11	File Creation	UserContext	Scoping for standard vs elevated or service accounts
AN1040	Windows	Execution of file enumeration commands (e.g., 'dir', 'tree') from non-standard processes or unusual user contexts, followed by recursive directory traversal or access to sensitive locations.	WinEventLog:Sysmon	EventCode=11	File Creation	TimeWindow	Defines burst activity over short periods (e.g., >50 directory queries in 30s)

Detection Strategies

Detection Strategy ID (DET0060)

Detection Strategy Name (Detect Ingress Tool Transfers via Behavioral Chain)

Analytic (AN0165 to AN0165)

Analytic Elements

AN	Platform	Detection Statement	Data Component Elements (DC)			Mutable Elements	
			Name	Channel	Data Component	Field	Description
AN0165	Windows	Unusual or uncommon processes initiate network connections to external destinations followed by file creation (tools downloaded).	WinEventLog:Sysmon	EventCode=3, 22	Network Connection Creation	ParentProcessName	Tune for known good updaters (e.g., ChromeUpdate, OneDrive)
AN0165	Windows	Unusual or uncommon processes initiate network connections to external destinations followed by file creation (tools downloaded).	WinEventLog:Sysmon	EventCode=3, 22	Network Connection Creation	DestinationIPCategory	Allow filtering by internal vs external IP blocks
AN0165	Windows	Unusual or uncommon processes initiate network connections to external destinations followed by file creation (tools downloaded).	WinEventLog:Sysmon	EventCode=3, 22	Network Connection Creation	FilePathRegex	Focus on uncommon file drop paths (e.g., C:\Users\Public\)
AN0165	Windows	Unusual or uncommon processes initiate network connections to external destinations followed by file creation (tools downloaded).	WinEventLog:Sysmon	EventCode=11	File Creation	ParentProcessName	Tune for known good updaters (e.g., ChromeUpdate, OneDrive)
AN0165	Windows	Unusual or uncommon processes initiate network connections to external destinations followed by file creation (tools downloaded).	WinEventLog:Sysmon	EventCode=11	File Creation	DestinationIPCategory	Allow filtering by internal vs external IP blocks
AN0165	Windows	Unusual or uncommon processes initiate network connections to external destinations followed by file creation (tools downloaded).	WinEventLog:Sysmon	EventCode=11	File Creation	FilePathRegex	Focus on uncommon file drop paths (e.g., C:\Users\Public\)
AN0165	Windows	Unusual or uncommon processes initiate network connections to external destinations followed by file creation (tools downloaded).	WinEventLog:Sysmon	EventCode=1	Process Creation	ParentProcessName	Tune for known good updaters (e.g., ChromeUpdate, OneDrive)
AN0165	Windows	Unusual or uncommon processes initiate network connections to external destinations followed by file creation (tools downloaded).	WinEventLog:Sysmon	EventCode=1	Process Creation	DestinationIPCategory	Allow filtering by internal vs external IP blocks
AN0165	Windows	Unusual or uncommon processes initiate network connections to external destinations followed by file creation (tools downloaded).	WinEventLog:Sysmon	EventCode=1	Process Creation	FilePathRegex	Focus on uncommon file drop paths (e.g., C:\Users\Public\)

Detection Strategies

Detection Strategy ID (DET0365)

Detection Strategy Name (Detect Registry and Startup Folder Persistence (Windows))

Analytic (AN1032 to AN1032)

Analytic Elements

AN	Platform	Detection Statement	Data Component Elements (DC)			Mutable Elements	
			Name	Channel	Data Component	Field	Description
AN1032	Windows	Correlation of Registry key creation/modification events under known Run/Startup keys with new or unusual binary paths or script-based payloads. Multi-event detection includes registry modification followed by process execution from non-standard directories or abnormal parent-child process relationships.	WinEventLog:Sysmon	EventCode=1	Process Creation	ImagePath	Full path of the binary/script being registered in Run keys. Tunable to exclude known software baselines.
AN1032	Windows	Correlation of Registry key creation/modification events under known Run/Startup keys with new or unusual binary paths or script-based payloads. Multi-event detection includes registry modification followed by process execution from non-standard directories or abnormal parent-child process relationships.	WinEventLog:Sysmon	EventCode=1	Process Creation	RegistryKeyPath	Tunable list of startup-related registry keys to monitor more/less aggressively based on enterprise software context.
AN1032	Windows	Correlation of Registry key creation/modification events under known Run/Startup keys with new or unusual binary paths or script-based payloads. Multi-event detection includes registry modification followed by process execution from non-standard directories or abnormal parent-child process relationships.	WinEventLog:Sysmon	EventCode=1	Process Creation	TimeWindow	Correlate registry key creation and process execution within this window. Defaults between 5–10 minutes.
AN1032	Windows	Correlation of Registry key creation/modification events under known Run/Startup keys with new or unusual binary paths or script-based payloads. Multi-event detection includes registry modification followed by process execution from non-standard directories or abnormal parent-child process relationships.	WinEventLog:Sysmon	EventCode=1	Process Creation	UserContext	Filter for specific user SIDs or exclude known admin/script accounts.
AN1032	Windows	Correlation of Registry key creation/modification events under known Run/Startup keys with new or unusual binary paths or script-based payloads. Multi-event detection includes registry modification followed by process execution from non-standard directories or abnormal parent-child process relationships.	WinEventLog:Sysmon	EventCode=13, 14	Windows Registry Key Modification	ImagePath	Full path of the binary/script being registered in Run keys. Tunable to exclude known software baselines.

AN	Platform	Detection Statement	Data Component Elements (DC)			Mutable Elements	
			Name	Channel	Data Component	Field	Description
AN1032	Windows	Correlation of Registry key creation/modification events under known Run/Startup keys with new or unusual binary paths or script-based payloads. Multi-event detection includes registry modification followed by process execution from non-standard directories or abnormal parent-child process relationships.	WinEventLog:Sysmon	EventCode=13, 14	Windows Registry Key Modification	RegistryKeyPath	Tunable list of startup-related registry keys to monitor more/less aggressively based on enterprise software context.
AN1032	Windows	Correlation of Registry key creation/modification events under known Run/Startup keys with new or unusual binary paths or script-based payloads. Multi-event detection includes registry modification followed by process execution from non-standard directories or abnormal parent-child process relationships.	WinEventLog:Sysmon	EventCode=13, 14	Windows Registry Key Modification	TimeWindow	Correlate registry key creation and process execution within this window. Defaults between 5–10 minutes.
AN1032	Windows	Correlation of Registry key creation/modification events under known Run/Startup keys with new or unusual binary paths or script-based payloads. Multi-event detection includes registry modification followed by process execution from non-standard directories or abnormal parent-child process relationships.	WinEventLog:Sysmon	EventCode=13, 14	Windows Registry Key Modification	UserContext	Filter for specific user SIDs or exclude known admin/script accounts.
AN1032	Windows	Correlation of Registry key creation/modification events under known Run/Startup keys with new or unusual binary paths or script-based payloads. Multi-event detection includes registry modification followed by process execution from non-standard directories or abnormal parent-child process relationships.	WinEventLog:Microsoft-Windows-Shell-Core	New startup folder shortcut or binary placed in Startup directory	File Creation	ImagePath	Full path of the binary/script being registered in Run keys. Tunable to exclude known software baselines.
AN1032	Windows	Correlation of Registry key creation/modification events under known Run/Startup keys with new or unusual binary paths or script-based payloads. Multi-event detection includes registry modification followed by process execution from non-standard directories or abnormal parent-child process relationships.	WinEventLog:Microsoft-Windows-Shell-Core	New startup folder shortcut or binary placed in Startup directory	File Creation	RegistryKeyPath	Tunable list of startup-related registry keys to monitor more/less aggressively based on enterprise software context.

AN	Platform	Detection Statement	Data Component Elements (DC)			Mutable Elements	
			Name	Channel	Data Component	Field	Description
AN1032	Windows	Correlation of Registry key creation/modification events under known Run/Startup keys with new or unusual binary paths or script-based	WinEventLog:Microsoft-Windows-Sh	New startup folder shortcut or binary placed in	File Creation	TimeWindow	Correlate registry key creation and process execution within this

AN	Platform	Detection Statement	Data Component Elements (DC)			Mutable Elements	
			Name	Channel	Data Component	Field	Description
		payloads. Multi-event detection includes registry modification followed by process execution from non-standard directories or abnormal parent-child process relationships.	ell-Core	Startup directory			window. Defaults between5–10 minutes.
AN1032	Windows	Correlation of Registry key creation/modification events under known Run/Startup keys with new or unusual binary paths or script-based payloads. Multi-event detection includes registry modification followed by process execution from non-standard directories or abnormal parent-child process relationships.	WinEventLog:Microsoft-Windows-Shell-Core	New startup folder shortcut or binary placed in Startup directory	File Creation	UserContext	Filter for specific user SIDs or exclude known admin/script accounts.

Detection Strategies

Detection Strategy ID (DET0110)

Detection Strategy Name (Setuid/Setgid Privilege Abuse Detection (Linux/macOS))

Analytic (AN0307 to AN0307)

Analytic Elements

AN	Platform	Detection Statement	Data Component Elements (DC)			Mutable Elements	
			Name	Channel	Data Component	Field	Description
AN0307	Linux	Correlation of chmod operations setting setuid/setgid bits followed by privileged process execution (EUID != UID), especially from user-writable or abnormal paths.	auditd:SYSCALL	chmod, execve	Command Execution	UserContext	Track execution of setuid binaries where UID != EUID or executed from unexpected user context
AN0307	Linux	Correlation of chmod operations setting setuid/setgid bits followed by privileged process execution (EUID != UID), especially from user-writable or abnormal paths.	auditd:SYSCALL	chmod, execve	Command Execution	FilePathScope	Restrict detection to non-standard locations (e.g., /tmp, /home/*, /var/tmp)
AN0307	Linux	Correlation of chmod operations setting setuid/setgid bits followed by privileged process execution (EUID != UID), especially from user-writable or abnormal paths.	auditd:SYSCALL	chmod, execve	Command Execution	TimeWindow	Time delta between chmod setting setuid/gid and process execution to define a suspicious window
AN0307	Linux	Correlation of chmod operations setting setuid/setgid bits followed by privileged process execution (EUID != UID), especially from user-writable or abnormal paths.	auditd:SYSCALL	execve	Process Creation	UserContext	Track execution of setuid binaries where UID != EUID or executed from unexpected user context
AN0307	Linux	Correlation of chmod operations setting setuid/setgid bits followed by privileged process execution (EUID != UID), especially from user-writable or abnormal paths.	auditd:SYSCALL	execve	Process Creation	FilePathScope	Restrict detection to non-standard locations (e.g., /tmp, /home/*, /var/tmp)
AN0307	Linux	Correlation of chmod operations setting setuid/setgid bits followed by privileged process execution (EUID != UID), especially from user-writable or abnormal paths.	auditd:SYSCALL	execve	Process Creation	TimeWindow	Time delta between chmod setting setuid/gid and process execution to define a suspicious window

Detection Strategies

Detection Strategy ID (DET0298)

Detection Strategy Name (Detect Archiving via Utility (T1560.001))

Analytic (AN0831 to AN0831)

Analytic Elements

AN	Platform	Detection Statement	Data Component Elements (DC)			Mutable Elements	
			Name	Channel	Data Component	Field	Description
AN0831	Windows	Detects adversarial archiving using built-in or third-party utilities (makecab, diantz, xcopy, certutil, 7z, WinRAR, WinZip). Correlates suspicious process creation events with command-line arguments for compression/encoding, followed by creation of archive files (.cab, .zip, .7z, .rar). Identifies anomalous loading of crypt32.dll for encryption operations or execution of diantz.exe to compress remotely staged files.	WinEventLog:Security	EventCode=4688	Process Creation	SuspiciousExtensions	List of archive extensions considered high risk (.cab, .zip, .7z, .rar).
AN0831	Windows	Detects adversarial archiving using built-in or third-party utilities (makecab, diantz, xcopy, certutil, 7z, WinRAR, WinZip). Correlates suspicious process creation events with command-line arguments for compression/encoding, followed by creation of archive files (.cab, .zip, .7z, .rar). Identifies anomalous loading of crypt32.dll for encryption operations or execution of diantz.exe to compress remotely staged files.	WinEventLog:Security	EventCode=4688	Process Creation	ProcessAllowlist	Known business utilities allowed to create archives without alerting.
AN0831	Windows	Detects adversarial archiving using built-in or third-party utilities (makecab, diantz, xcopy, certutil, 7z, WinRAR, WinZip). Correlates suspicious process creation events with command-line arguments for compression/encoding, followed by creation of archive files (.cab, .zip, .7z, .rar). Identifies anomalous loading of crypt32.dll for encryption operations or execution of diantz.exe to compress remotely staged files.	WinEventLog:Security	EventCode=4688	Process Creation	FileSizeThresholdMB	Minimum archive size threshold to filter out benign small compressions.

AN	Platform	Detection Statement	Data Component Elements (DC)			Mutable Elements	
			Name	Channel	Data Component	Field	Description
AN0831	Windows	Detects adversarial archiving using built-in or third-party utilities (makecab, diantz, xcopy, certutil, 7z, WinRAR, WinZip). Correlates suspicious process creation events with command-line arguments for compression/encoding, followed by creation of archive files (.cab, .zip, .7z, .rar). Identifies	WinEventLog:Sysmon	EventCode=11	File Creation	SuspiciousExtensions	List of archive extensions considered high risk (.cab, .zip, .7z, .rar).

AN	Platform	Detection Statement	Data Component Elements (DC)			Mutable Elements	
			Name	Channel	Data Component	Field	Description
		anomalous loading of crypt32.dll for encryption operations or execution of diantz.exe to compress remotely staged files.					
AN0831	Windows	Detects adversarial archiving using built-in or third-party utilities (makecab, diantz, xcopy, certutil, 7z, WinRAR, WinZip). Correlates suspicious process creation events with command-line arguments for compression/encoding, followed by creation of archive files (.cab, .zip, .7z, .rar). Identifies anomalous loading of crypt32.dll for encryption operations or execution of diantz.exe to compress remotely staged files.	WinEventLog:Sysmon	EventCode=11	File Creation	ProcessAllowlist	Known business utilities allowed to create archives without alerting.
AN0831	Windows	Detects adversarial archiving using built-in or third-party utilities (makecab, diantz, xcopy, certutil, 7z, WinRAR, WinZip). Correlates suspicious process creation events with command-line arguments for compression/encoding, followed by creation of archive files (.cab, .zip, .7z, .rar). Identifies anomalous loading of crypt32.dll for encryption operations or execution of diantz.exe to compress remotely staged files.	WinEventLog:Sysmon	EventCode=11	File Creation	FileSizeThresholdMB	Minimum archive size threshold to filter out benign small compressions.
AN0831	Windows	Detects adversarial archiving using built-in or third-party utilities (makecab, diantz, xcopy, certutil, 7z, WinRAR, WinZip). Correlates suspicious process creation events with command-line arguments for compression/encoding, followed by creation of archive files (.cab, .zip, .7z, .rar). Identifies anomalous loading of crypt32.dll for encryption operations or execution of diantz.exe to compress remotely staged files.	WinEventLog:Sysmon	EventCode=7	Module Load	SuspiciousExtensions	List of archive extensions considered high risk (.cab, .zip, .7z, .rar).
AN0831	Windows	Detects adversarial archiving using built-in or third-party utilities (makecab, diantz, xcopy, certutil, 7z, WinRAR, WinZip). Correlates suspicious process creation events with command-line arguments for compression/encoding, followed by creation of archive files (.cab, .zip, .7z, .rar). Identifies anomalous loading of crypt32.dll for encryption operations or execution of diantz.exe to compress remotely staged files.	WinEventLog:Sysmon	EventCode=7	Module Load	ProcessAllowlist	Known business utilities allowed to create archives without alerting.

AN	Platform	Detection Statement	Data Component Elements (DC)			Mutable Elements	
			Name	Channel	Data Component	Field	Description
AN0831	Windows	Detects adversarial archiving using built-in or third-party utilities (makecab, diantz, xcopy, certutil, 7z, WinRAR, WinZip). Correlates suspicious process creation events with command-line arguments for compression/encoding, followed by creation of archive files (.cab, .zip, .7z, .rar). Identifies anomalous loading of crypt32.dll for encryption operations or execution of diantz.exe to compress remotely staged files.	WinEventLog:Sysmon	EventCode=7	Module Load	FileSizeThresholdMB	Minimum archive size threshold to filter out benign small compressions.