List of covered sigma rules

Title: Windows PowerShell User Agent
- description: Detects Windows PowerShell Web Access
- category: data/rules/proxy
- level: medium
- id: c8557060-9221-4448-8794-96320e6f3e74

Title: Download from Suspicious Dyndns Hosts
- description: Detects download of certain file types from hosts with dynamic DNS names (selected list)
- category: data/rules/proxy
- level: medium
- id: 195c1119-ef07-4909-bb12-e66f5e07bf3c

Title: Suspicious User Agent
- description: Detects suspicious malformed user agent strings in proxy logs
- category: data/rules/proxy
- level: high
- id: 7195a772-4b3f-43a4-a210-6a003d65caa1

Title: Malware User Agent
- description: Detects suspicious user agent strings used by malware in proxy logs
- category: data/rules/proxy
- level: high
- id: 5c84856b-55a5-45f1-826f-13f37250cf4e

Title: Download EXE from Suspicious TLD
- description: Detects executable downloads from suspicious remote systems
- category: data/rules/proxy
- level: low
- id: b5de2919-b74a-4805-91a7-5049accbaefe

Title: Domestic Kitten FurBall Malware Pattern
- description: Detects specific malware patterns used by FurBall malware linked to Iranian Domestic Kitten APT group
- category: data/rules/proxy
- level: high
- id: 6c939dfa-c710-4e12-a4dd-47e1f10e68e1

Title: CobaltStrike Malleable (OCSP) Profile
- description: Detects Malleable (OCSP) Profile with Typo (OSCP) in URL
- category: data/rules/proxy
- level: high
- id: 37325383-740a-403d-b1a2-b2b4ab7992e7

Title: Flash Player Update from Suspicious Location
- description: Detects a flashplayer update from an unofficial location
- category: data/rules/proxy
- level: high
- id: 4922a5dd-6743-4fc2-8e81-144374280997

Title: CobaltStrike Malleable OneDrive Browsing Traffic Profile
- description: Detects Malleable OneDrive Profile
- category: data/rules/proxy
- level: high
- id: c9b33401-cc6a-4cf6-83bb-57ddcb2407fc

Title: Chafer Malware URL Pattern
- description: Detects HTTP requests used by Chafer malware
- category: data/rules/proxy
- level: critical
- id: fb502828-2db0-438e-93e6-801c7548686d

Title: APT User Agent
- description: Detects suspicious user agent strings used in APT malware in proxy logs
- category: data/rules/proxy
- level: high
- id: 6ec820f2-e963-4801-9127-d8b2dce4d31b

Title: iOS Implant URL Pattern

- description: Detects URL pattern used by iOS Implant
- category: data/rules/proxy
- level: critical
- id: e06ac91d-b9e6-443d-8e5b-af749e7aa6b6

Title: Download from Suspicious TLD
- description: Detects download of certain file types from hosts in suspicious TLDs
- category: data/rules/proxy
- level: low
- id: 00d0b5ab-1f55-4120-8e83-487c0a7baf19

Title: BabyShark Agent Pattern
- description: Detects Baby Shark C2 Framework communication patterns
- category: data/rules/proxy
- level: critical
- id: 304810ed-8853-437f-9e36-c4975c3dfd7e

Title: Empty User Agent
- description: Detects suspicious empty user agent strings in proxy logs
- category: data/rules/proxy
- level: medium
- id: 21e44d78-95e7-421b-a464-ffd8395659c4

Title: Windows WebDAV User Agent
- description: Detects WebDav DownloadCradle
- category: data/rules/proxy
- level: high
- id: e09aed7a-09e0-4c9a-90dd-f0d52507347e

Title: Bitsadmin to Uncommon TLD
- description: Detects Bitsadmin connections to domains with uncommon TLDs - https://twitter.com/jhencinski/status/11026951184
- category: data/rules/proxy
- level: high
- id: 9eb68894-7476-4cd6-8752-23b51f5883a7

Title: Ursnif Malware Download URL Pattern
- description: Detects download of Ursnif malware done by dropper documents.
- category: data/rules/proxy
- level: critical
- id: a36ce77e-30db-4ea0-8795-644d7af5dfb4

Title: Turla ComRAT
- description: Detects Turla ComRAT patterns
- category: data/rules/proxy
- level: critical
- id: 7857f021-007f-4928-8b2c-7aedbe64bb82

Title: Raw Paste Service Access
- description: Detects direct access to raw pastes in different paste services often used by malware in their second stages to
- category: data/rules/proxy
- level: high
- id: 5468045b-4fcc-4d1a-973c-c9c9578edacb

Title: Empire UserAgent URI Combo
- description: Detects user agent and URI paths used by empire agents
- category: data/rules/proxy
- level: high
- id: b923f7d6-ac89-4a50-a71a-89fb846b4aa8

Title: PwnDrp Access
- description: Detects downloads from PwnDrp web servers developed for red team testing and most likely also used for criminal
- category: data/rules/proxy
- level: critical
- id: 2b1ee7e4-89b6-4739-b7bb-b811b6607e5e

Title: CobaltStrike Malleable Amazon Browsing Traffic Profile
- description: Detects Malleable Amazon Profile
- category: data/rules/proxy
- level: high

- id: 953b895e-5cc9-454b-b183-7f3db555452e

Title: Crypto Miner User Agent
- description: Detects suspicious user agent strings used by crypto miners in proxy logs
- category: data/rules/proxy
- level: high
- id: fa935401-513b-467b-81f4-f9e77aa0dd78

Title: Java Class Proxy Download
- description: Detects Java class download in proxy logs, e.g. used in Log4shell exploitation attacks against Log4j.
- category: data/rules/proxy
- level: high
- id: 53c15703-b04c-42bb-9055-1937ddfb3392

Title: APT40 Dropbox Tool User Agent
- description: Detects suspicious user agent string of APT40 Dropbox tool
- category: data/rules/proxy
- level: high
- id: 5ba715b6-71b7-44fd-8245-f66893e81b3d

Title: Exploit Framework User Agent
- description: Detects suspicious user agent strings used by exploit / pentest frameworks like Metasploit in proxy logs
- category: data/rules/proxy
- level: high
- id: fdd1bfb5-f60b-4a35-910e-f36ed3d0b32f

Title: CobaltStrike Malformed UAs in Malleable Profiles
- description: Detects different malformed user agents used in Malleable Profiles used with Cobalt Strike
- category: data/rules/proxy
- level: critical
- id: 41b42a36-f62c-4c34-bd40-8cb804a34ad8

Title: Telegram API Access
- description: Detects suspicious requests to Telegram API without the usual Telegram User-Agent
- category: data/rules/proxy
- level: medium
- id: b494b165-6634-483d-8c47-2026a6c52372

Title: Hack Tool User Agent
- description: Detects suspicious user agent strings user by hack tools in proxy logs
- category: data/rules/proxy
- level: high
- id: c42a3073-30fb-48ae-8c99-c23ada84b103

Title: Ursnif Malware C2 URL Pattern
- description: Detects Ursnif C2 traffic.
- category: data/rules/proxy
- level: critical
- id: 932ac737-33ca-4afd-9869-0d48b391fcc9

Title: Screen Capture - macOS
- description: Detects attempts to use screencapture to collect macOS screenshots
- category: data/rules/macos/process_creation
- level: low
- id: 0877ed01-da46-4c49-8476-d49cdd80dfa7

Title: Credentials In Files
- description: Detecting attempts to extract passwords with grep and laZagne
- category: data/rules/macos/process_creation
- level: high
- id: 53b1b378-9b06-4992-b972-dde6e423d2b4

Title: MacOS Scripting Interpreter AppleScript
- description: Detects execution of AppleScript of the macOS scripting language AppleScript.
- category: data/rules/macos/process_creation
- level: medium
- id: 1bc2e6c5-0885-472b-bed6-be5ea8eace55

Title: System Network Discovery - macOS

- description: Detects enumeration of local network configuration
- category: data/rules/macos/process_creation
- level: informational
- id: 58800443-f9fc-4d55-ae0c-98a3966dfb97

Title: Macos Remote System Discovery
- description: Detects the enumeration of other remote systems.
- category: data/rules/macos/process_creation
- level: informational
- id: 10227522-8429-47e6-a301-f2b2d014e7ad

Title: Hidden User Creation
- description: Detects creation of a hidden user account on macOS (UserID < 500) or with IsHidden option
- category: data/rules/macos/process_creation
- level: medium
- id: b22a5b36-2431-493a-8be1-0bae56c28ef3

Title: Indicator Removal on Host - Clear Mac System Logs
- description: Detects deletion of local audit logs
- category: data/rules/macos/process_creation
- level: medium
- id: acf61bd8-d814-4272-81f0-a7a269aa69aa

Title: Security Software Discovery
- description: Detects usage of system utilities (only grep for now) to discover security software discovery
- category: data/rules/macos/process_creation
- level: medium
- id: 0ed75b9c-c73b-424d-9e7d-496cd565fbe0

Title: Decode Base64 Encoded Text
- description: Detects usage of base64 utility to decode arbitrary base64-encoded text
- category: data/rules/macos/process_creation
- level: low
- id: 719c22d7-c11a-4f2c-93a6-2cfdd5412f68

Title: System Shutdown/Reboot
- description: Adversaries may shutdown/reboot systems to interrupt access to, or aid in the destruction of, those systems.
- category: data/rules/macos/process_creation
- level: informational
- id: 40b1fbe2-18ea-4ee7-be47-0294285811de

Title: Scheduled Cron Task/Job
- description: Detects abuse of the cron utility to perform task scheduling for initial or recurring execution of malicious co
- category: data/rules/macos/process_creation
- level: medium
- id: 7c3b43d8-d794-47d2-800a-d277715aa460

Title: Space After Filename - macOS
- description: Detects attempts to masquerade as legitimate files by adding a space to the end of the filename.
- category: data/rules/macos/process_creation
- level: low
- id: b6e2a2e3-2d30-43b1-a4ea-071e36595690

Title: Creation Of A Local User Account
- description: Detects the creation of a new user account. Such accounts may be used for persistence that do not require persi
- category: data/rules/macos/process_creation
- level: low
- id: 51719bf5-e4fd-4e44-8ba8-b830e7ac0731

Title: File Time Attribute Change
- description: Detect file time attribute change to hide new or changes to existing files.
- category: data/rules/macos/process_creation
- level: medium
- id: 88c0f9d8-30a8-4120-bb6b-ebb54abcf2a0

Title: Local Groups Discovery
- description: Detects enumeration of local system groups
- category: data/rules/macos/process_creation
- level: informational

- id: 89bb1f97-c7b9-40e8-b52b-7d6afbd67276

Title: System Network Connections Discovery
- description: Detects usage of system utilities to discover system network connections
- category: data/rules/macos/process_creation
- level: informational
- id: 9a7a0393-2144-4626-9bf1-7c2f5a7321db

Title: Split A File Into Pieces
- description: Detection use of the command "split" to split files into parts and possible transfer.
- category: data/rules/macos/process_creation
- level: low
- id: 7f2bb9d5-6395-4de5-969c-70c11fbe6b12

Title: MacOS Network Service Scanning
- description: Detects enumeration of local or remote network services.
- category: data/rules/macos/process_creation
- level: low
- id: 84bae5d4-b518-4ae0-b331-6d4afd34d00f

Title: Network Sniffing
- description: Detects the usage of tooling to sniff network traffic. An adversary may place a network interface into promiscu
- category: data/rules/macos/process_creation
- level: informational
- id: adc9bcc4-c39c-4f6b-a711-1884017bf043

Title: GUI Input Capture - macOS
- description: Detects attempts to use system dialog prompts to capture user credentials
- category: data/rules/macos/process_creation
- level: low
- id: 60f1ce20-484e-41bd-85f4-ac4afec2c541

Title: Local System Accounts Discovery
- description: Detects enumeration of local systeam accounts on MacOS
- category: data/rules/macos/process_creation
- level: low
- id: ddf36b67-e872-4507-ab2e-46bda21b842c

Title: File and Directory Discovery
- description: Detects usage of system utilities to discover files and directories
- category: data/rules/macos/process_creation
- level: informational
- id: 089dbdf6-b960-4bcc-90e3-ffc3480c20f6

Title: Suspicious History File Operations
- description: Detects commandline operations on shell history files
- category: data/rules/macos/process_creation
- level: medium
- id: 508a9374-ad52-4789-b568-fc358def2c65

Title: Gatekeeper Bypass via Xattr
- description: Detects macOS Gatekeeper bypass via xattr utility
- category: data/rules/macos/process_creation
- level: low
- id: f5141b6d-9f42-41c6-a7bf-2a780678b29b

Title: Credentials from Password Stores - Keychain
- description: Detects passwords dumps from Keychain
- category: data/rules/macos/process_creation
- level: medium
- id: b120b587-a4c2-4b94-875d-99c9807d6955

Title: Binary Padding
- description: Adversaries may use binary padding to add junk data and change the on-disk representation of malware. This rule
- category: data/rules/macos/process_creation
- level: high
- id: 95361ce5-c891-4b0a-87ca-e24607884a96

Title: Suspicious MacOS Firmware Activity

- description: Detects when a user manipulates with Firmward Password on MacOS. NOTE - this command has been disabled on silic
- category: data/rules/macos/process_creation
- level: medium
- id: 7ed2c9f7-c59d-4c82-a7e2-f859aa676099

Title: Disable Security Tools
- description: Detects disabling security tools
- category: data/rules/macos/process_creation
- level: medium
- id: ff39f1a6-84ac-476f-a1af-37fcdf53d7c0

Title: Startup Items
- description: Detects creation of startup item plist files that automatically get executed at boot initialization to establis
- category: data/rules/macos/file_event
- level: low
- id: dfe8b941-4e54-4242-b674-6b613d521962

Title: MacOS Emond Launch Daemon
- description: Detects additions to the Emond Launch Daemon that adversaries may use to gain persistence and elevate privilege
- category: data/rules/macos/file_event
- level: medium
- id: 23c43900-e732-45a4-8354-63e4a6c187ce

Title: Okta Policy Modified or Deleted
- description: Detects when an Okta policy is modified or deleted.
- category: data/rules/cloud/okta
- level: low
- id: 1667a172-ed4c-463c-9969-efd92195319a

Title: Okta Security Threat Detected
- description: Detects when an security threat is detected in Okta.
- category: data/rules/cloud/okta
- level: medium
- id: 5c82f0b9-3c6d-477f-a318-0e14a1df73e0

Title: Okta MFA Reset or Deactivated
- description: Detects when an attempt at deactivating or resetting MFA.
- category: data/rules/cloud/okta
- level: medium
- id: 50e068d7-1e6b-4054-87e5-0a592c40c7e0

Title: Okta Admin Role Assigned to an User or Group
- description: Detects when an the Administrator role is assigned to an user or group.
- category: data/rules/cloud/okta
- level: medium
- id: 413d4a81-6c98-4479-9863-014785fd579c

Title: Okta Application Sign-On Policy Modified or Deleted
- description: Detects when an application Sign-on Policy is modified or deleted.
- category: data/rules/cloud/okta
- level: medium
- id: 8f668cc4-c18e-45fe-ad00-624a981cf88a

Title: Okta Policy Rule Modified or Deleted
- description: Detects when an Policy Rule is Modified or Deleted.
- category: data/rules/cloud/okta
- level: medium
- id: 0c97c1d3-4057-45c9-b148-1de94b631931

Title: Okta API Token Revoked
- description: Detects when a API Token is revoked.
- category: data/rules/cloud/okta
- level: medium
- id: cf1dbc6b-6205-41b4-9b88-a83980d2255b

Title: Okta Unauthorized Access to App
- description: Detects when unauthorized access to app occurs.
- category: data/rules/cloud/okta
- level: medium

- id: 6cc2b61b-d97e-42ef-a9dd-8aa8dc951657

Title: Okta API Token Created
- description: Detects when a API token is created
- category: data/rules/cloud/okta
- level: medium
- id: 19951c21-229d-4ccb-8774-b993c3ff3c5c

Title: Okta Network Zone Deactivated or Deleted
- description: Detects when an Network Zone is Deactivated or Deleted.
- category: data/rules/cloud/okta
- level: medium
- id: 9f308120-69ed-4506-abde-ac6da81f4310

Title: Okta User Account Locked Out
- description: Detects when an user account is locked out.
- category: data/rules/cloud/okta
- level: medium
- id: 14701da0-4b0f-4ee6-9c95-2ffb4e73bb9a

Title: Okta Application Modified or Deleted
- description: Detects when an application is modified or deleted.
- category: data/rules/cloud/okta
- level: medium
- id: 7899144b-e416-4c28-b0b5-ab8f9e0a541d

Title: Suspicious Inbox Forwarding
- description: Detects when a Microsoft Cloud App Security reported suspicious email forwarding rules, for example, if a user
- category: data/rules/cloud/m365
- level: low
- id: 6c220477-0b5b-4b25-bb90-66183b4089e8

Title: Activity from Suspicious IP Addresses
- description: Detects when a Microsoft Cloud App Security reported users were active from an IP address identified as risky b
- category: data/rules/cloud/m365
- level: medium
- id: a3501e8e-af9e-43c6-8cd6-9360bdaae498

Title: Microsoft 365 - Impossible Travel Activity
- description: Detects when a Microsoft Cloud App Security reported a risky sign-in attempt due to a login associated with an
- category: data/rules/cloud/m365
- level: medium
- id: d7eab125-5f94-43df-8710-795b80fa1189

Title: Activity Performed by Terminated User
- description: Detects when a Microsoft Cloud App Security reported for users whose account were terminated in Azure AD, but s
- category: data/rules/cloud/m365
- level: medium
- id: 2e669ed8-742e-4fe5-b3c4-5a59b486c2ee

Title: Logon from a Risky IP Address
- description: Detects when a Microsoft Cloud App Security reported when a user signs into your sanctioned apps from a risky I
- category: data/rules/cloud/m365
- level: medium
- id: c191e2fa-f9d6-4ccf-82af-4f2aba08359f

Title: Microsoft 365 - User Restricted from Sending Email
- description: Detects when a Security Compliance Center reported a user who exceeded sending limits of the service policies a
- category: data/rules/cloud/m365
- level: medium
- id: ff246f56-7f24-402a-baca-b86540e3925c

Title: Suspicious OAuth App File Download Activities
- description: Detects when a Microsoft Cloud App Security reported when an app downloads multiple files from Microsoft ShareP
- category: data/rules/cloud/m365
- level: medium
- id: ee111937-1fe7-40f0-962a-0eb44d57d174

Title: Activity from Anonymous IP Addresses

- description: Detects when a Microsoft Cloud App Security reported when users were active from an IP address that has been id
- category: data/rules/cloud/m365
- level: medium
- id: d8b0a4fe-07a8-41be-bd39-b14afa025d95

Title: Data Exfiltration to Unsanctioned Apps
- description: Detects when a Microsoft Cloud App Security reported when a user or IP address uses an app that is not sanction
- category: data/rules/cloud/m365
- level: medium
- id: 2b669496-d215-47d8-bd9a-f4a45bf07cda

Title: Microsoft 365 - Potential Ransomware Activity
- description: Detects when a Microsoft Cloud App Security reported when a user uploads files to the cloud that might be infec
- category: data/rules/cloud/m365
- level: medium
- id: bd132164-884a-48f1-aa2d-c6d646b04c69

Title: New Federated Domain Added
- description: Alert for the addition of a new federated domain.
- category: data/rules/cloud/m365
- level: medium
- id: 42127bdd-9133-474f-a6f1-97b6c08a4339

Title: Microsoft 365 - Unusual Volume of File Deletion
- description: Detects when a Microsoft Cloud App Security reported a user has deleted a unusual a large volume of files.
- category: data/rules/cloud/m365
- level: medium
- id: 78a34b67-3c39-4886-8fb4-61c46dc18ecd

Title: Activity from Infrequent Country
- description: Detects when a Microsoft Cloud App Security reported when an activity occurs from a location that wasn't recent
- category: data/rules/cloud/m365
- level: medium
- id: 0f2468a2-5055-4212-a368-7321198ee706

Title: Azure Suppression Rule Created
- description: Identifies when a suppression rule is created in Azure. Adversary's could attempt this to evade detection.
- category: data/rules/cloud/azure
- level: medium
- id: 92cc3e5d-eb57-419d-8c16-5c63f325a401

Title: Multifactor Authentication Denied
- description: User has indicated they haven't instigated the MFA prompt and could indicate an attacker has the password for t
- category: data/rules/cloud/azure
- level: medium
- id: e40f4962-b02b-4192-9bfe-245f7ece1f99

Title: Azure Application Gateway Modified or Deleted
- description: Identifies when a application gateway is modified or deleted.
- category: data/rules/cloud/azure
- level: medium
- id: ad87d14e-7599-4633-ba81-aeb60cfe8cd6

Title: Azure New CloudShell Created
- description: Identifies when a new cloudshell is created inside of Azure portal.
- category: data/rules/cloud/azure
- level: medium
- id: 72af37e2-ec32-47dc-992b-bc288a2708cb

Title: Azure Owner Removed From Application or Service Principal
- description: Identifies when a owner is was removed from a application or service principal in Azure.
- category: data/rules/cloud/azure
- level: medium
- id: 636e30d5-3736-42ea-96b1-e6e2f8429fd6

Title: Azure VPN Connection Modified or Deleted
- description: Identifies when a VPN connection is modified or deleted.
- category: data/rules/cloud/azure
- level: medium

- id: 61171ffc-d79c-4ae5-8e10-9323dba19cd3

Title: Azure Network Security Configuration Modified or Deleted
- description: Identifies when a network security configuration is modified or deleted.
- category: data/rules/cloud/azure
- level: medium
- id: d22b4df4-5a67-4859-a578-8c9a0b5af9df

Title: Azure DNS Zone Modified or Deleted
- description: Identifies when DNS zone is modified or deleted.
- category: data/rules/cloud/azure
- level: medium
- id: af6925b0-8826-47f1-9324-337507a0babd

Title: Azure Application Credential Modified
- description: Identifies when a application credential is modified.
- category: data/rules/cloud/azure
- level: medium
- id: cdeef967-f9a1-4375-90ee-6978c5f23974

Title: Azure Point-to-site VPN Modified or Deleted
- description: Identifies when a Point-to-site VPN is Modified or Deleted.
- category: data/rules/cloud/azure
- level: medium
- id: d9557b75-267b-4b43-922f-a775e2d1f792

Title: Azure Active Directory Hybrid Health AD FS Service Delete
- description: This detection uses azureactivity logs (Administrative category) to identify the deletion of an Azure AD Hybrid

A threat actor can create a new AD Health ADFS service and create a fake server to spoof AD FS signing logs. The health AD FS service can then be deleted after it is not longer needed via HTTP requests to Azure.

- category: data/rules/cloud/azure
- level: medium
- id: 48739819-8230-4ee3-a8ea-e0289d1fb0ff

Title: Azure Firewall Rule Configuration Modified or Deleted
- description: Identifies when a Firewall Rule Configuration is Modified or Deleted.
- category: data/rules/cloud/azure
- level: medium
- id: 2a7d64cf-81fa-4daf-ab1b-ab80b789c067

Title: Azure Virtual Network Modified or Deleted
- description: Identifies when a Virtual Network is modified or deleted in Azure.
- category: data/rules/cloud/azure
- level: medium
- id: bcfcc962-0e4a-4fd9-84bb-a833e672df3f

Title: Azure Kubernetes CronJob
- description: Identifies when a Azure Kubernetes CronJob runs in Azure Cloud. Kubernetes Job is a controller that creates one
- category: data/rules/cloud/azure
- level: medium
- id: 1c71e254-6655-42c1-b2d6-5e4718d7fc0a

Title: Azure Subscription Permission Elevation Via ActivityLogs
- description: Detects when a user has been elevated to manage all Azure Subscriptions. This change should be investigated imm
- category: data/rules/cloud/azure
- level: high
- id: 09438caa-07b1-4870-8405-1dbafe3dad95

Title: Azure Subscription Permission Elevation Via AuditLogs
- description: Detects when a user has been elevated to manage all Azure Subscriptions. This change should be investigated imm
- category: data/rules/cloud/azure
- level: high
- id: ca9bf243-465e-494a-9e54-bf9fc239057d

Title: Azure Unusual Authentication Interruption
- description: Detects when there is a interruption in the authentication process.
- category: data/rules/cloud/azure

- level: medium
- id: 8366030e-7216-476b-9927-271d79f13cf3

Title: Azure Firewall Modified or Deleted
- description: Identifies when a firewall is created, modified, or deleted.
- category: data/rules/cloud/azure
- level: medium
- id: 512cf937-ea9b-4332-939c-4c2c94baadcd

Title: Azure Network Firewall Policy Modified or Deleted
- description: Identifies when a Firewall Policy is Modified or Deleted.
- category: data/rules/cloud/azure
- level: medium
- id: 83c17918-746e-4bd9-920b-8e098bf88c23

Title: Azure Virtual Network Device Modified or Deleted
- description: Identifies when a virtual network device is being modified or deleted. This can be a network interface, network
- category: data/rules/cloud/azure
- level: medium
- id: 15ef3fac-f0f0-4dc4-ada0-660aa72980b3

Title: Change to Authentication Method
- description: Change to authentication method could be an indicated of an attacker adding an auth method to the account so th
- category: data/rules/cloud/azure
- level: medium
- id: 4d78a000-ab52-4564-88a5-7ab5242b20c7

Title: Azure Domain Federation Settings Modified
- description: Identifies when an user or application modified the federation settings on the domain.
- category: data/rules/cloud/azure
- level: medium
- id: 352a54e1-74ba-4929-9d47-8193d67aba1e

Title: Azure Kubernetes Service Account Modified or Deleted
- description: Identifies when a service account is modified or deleted.
- category: data/rules/cloud/azure
- level: medium
- id: 12d027c3-b48c-4d9d-8bb6-a732200034b2

Title: Azure Kubernetes Network Policy Change
- description: Identifies when a Azure Kubernetes network policy is modified or deleted.
- category: data/rules/cloud/azure
- level: medium
- id: 08d6ac24-c927-4469-b3b7-2e422d6e3c43

Title: Azure Service Principal Removed
- description: Identifies when a service principal was removed in Azure.
- category: data/rules/cloud/azure
- level: medium
- id: 448fd1ea-2116-4c62-9cde-a92d120e0f08

Title: Azure Kubernetes Admission Controller
- description: Identifies when an admission controller is executed in Azure Kubernetes. A Kubernetes Admission controller inte
- category: data/rules/cloud/azure
- level: medium
- id: a61a3c56-4ce2-4351-a079-88ae4cbd2b58

Title: Azure Kubernetes Cluster Created or Deleted
- description: Detects when a Azure Kubernetes Cluster is created or deleted.
- category: data/rules/cloud/azure
- level: low
- id: 9541f321-7cba-4b43-80fc-fbd1fb922808

Title: User Access Blocked by Azure Conditional Access
- description: Detect access has been blocked by Conditional Access policies. The access policy does not allow token issuance
- category: data/rules/cloud/azure
- level: medium
- id: 9a60e676-26ac-44c3-814b-0c2a8b977adf

Title: Disabled MFA to Bypass Authentication Mechanisms
- description: Detection for when multi factor authentication has been disabled, which might indicate a malicious activity to
- category: data/rules/cloud/azure
- level: medium
- id: 7ea78478-a4f9-42a6-9dcd-f861816122bf

Title: Azure Kubernetes RoleBinding/ClusterRoleBinding Modified and Deleted
- description: Detects the creation or patching of potential malicious RoleBinding/ClusterRoleBinding.
- category: data/rules/cloud/azure
- level: medium
- id: 25cb259b-bbdc-4b87-98b7-90d7c72f8743

Title: Azure Container Registry Created or Deleted
- description: Detects when a Container Registry is created or deleted.
- category: data/rules/cloud/azure
- level: low
- id: 93e0ef48-37c8-49ed-a02c-038aab23628e

Title: Azure Kubernetes Secret or Config Object Access
- description: Identifies when a Kubernetes account access a sensitive objects such as configmaps or secrets.
- category: data/rules/cloud/azure
- level: medium
- id: 7ee0b4aa-d8d4-4088-b661-20efdf41a04c

Title: Azure Device No Longer Managed or Compliant
- description: Identifies when a device in azure is no longer managed or compliant
- category: data/rules/cloud/azure
- level: medium
- id: 542b9912-c01f-4e3f-89a8-014c48cdca7d

Title: Granting Of Permissions To An Account
- description: Identifies IPs from which users grant access to other users on azure resources and alerts when a previously uns
- category: data/rules/cloud/azure
- level: medium
- id: a622fcd2-4b5a-436a-b8a2-a4171161833c

Title: Azure Kubernetes Events Deleted
- description: Detects when Events are deleted in Azure Kubernetes. An adversary may delete events in Azure Kubernetes in an a
- category: data/rules/cloud/azure
- level: medium
- id: 225d8b09-e714-479c-a0e4-55e6f29adf35

Title: Multifactor Authentication Interupted
- description: Identifies user login with multifactor authentication failures, which might be an indication an attacker has th
- category: data/rules/cloud/azure
- level: medium
- id: 5496ff55-42ec-4369-81cb-00f417029e25

Title: Azure Keyvault Secrets Modified or Deleted
- description: Identifies when secrets are modified or deleted in Azure.
- category: data/rules/cloud/azure
- level: medium
- id: b831353c-1971-477b-abb6-2828edc3bca1

Title: Azure Application Deleted
- description: Identifies when a application is deleted in Azure.
- category: data/rules/cloud/azure
- level: medium
- id: 410d2a41-1e6d-452f-85e5-abdd8257a823

Title: Azure Key Vault Modified or Deleted
- description: Identifies when a key vault is modified or deleted.
- category: data/rules/cloud/azure
- level: medium
- id: 459a2970-bb84-4e6a-a32e-ff0fbd99448d

Title: Azure Device or Configuration Modified or Deleted
- description: Identifies when a device or device configuration in azure is modified or deleted.
- category: data/rules/cloud/azure

- level: medium
- id: 46530378-f9db-4af9-a9e5-889c177d3881

Title: Azure Firewall Rule Collection Modified or Deleted
- description: Identifies when Rule Collections (Application, NAT, and Network) is being modified or deleted.
- category: data/rules/cloud/azure
- level: medium
- id: 025c9fe7-db72-49f9-af0d-31341dd7dd57

Title: User Added to an Administrator's Azure AD Role
- description: User Added to an Administrator's Azure AD Role
- category: data/rules/cloud/azure
- level: medium
- id: ebbeb024-5b1d-4e16-9c0c-917f86c708a7

Title: Azure Application Security Group Modified or Deleted
- description: Identifies when a application security group is modified or deleted.
- category: data/rules/cloud/azure
- level: medium
- id: 835747f1-9329-40b5-9cc3-97d465754ce6

Title: Azure Kubernetes Pods Deleted
- description: Identifies the deletion of Azure Kubernetes Pods.
- category: data/rules/cloud/azure
- level: medium
- id: b02f9591-12c3-4965-986a-88028629b2e1

Title: Azure Kubernetes Sensitive Role Access
- description: Identifies when ClusterRoles/Roles are being modified or deleted.
- category: data/rules/cloud/azure
- level: medium
- id: 818fee0c-e0ec-4e45-824e-83e4817b0887

Title: Azure Service Principal Created
- description: Identifies when a service principal is created in Azure.
- category: data/rules/cloud/azure
- level: medium
- id: 0ddcff6d-d262-40b0-804b-80eb592de8e3

Title: Azure Keyvault Key Modified or Deleted
- description: Identifies when a Keyvault Key is modified or deleted in Azure.
- category: data/rules/cloud/azure
- level: medium
- id: 80eeab92-0979-4152-942d-96749e11df40

Title: Azure Active Directory Hybrid Health AD FS New Server
- description: This detection uses azureactivity logs (Administrative category) to identify the creation or update of a server

A threat actor can create a new AD Health ADFS service and create a fake server instance to spoof AD FS signing logs. There is no need to compromise an on-prem AD FS server. This can be done programmatically via HTTP requests to Azure.

- category: data/rules/cloud/azure
- level: medium
- id: 288a39fc-4914-4831-9ada-270e9dc12cb4

Title: Account Lockout
- description: Identifies user account which has been locked because the user tried to sign in too many times with an incorrec
- category: data/rules/cloud/azure
- level: medium
- id: 2b7d6fc0-71ac-4cf7-8ed1-b5788ee5257a

Title: Number Of Resource Creation Or Deployment Activities
- description: Number of VM creations or deployment activities occur in Azure via the azureactivity log.
- category: data/rules/cloud/azure
- level: medium
- id: d2d901db-7a75-45a1-bc39-0cbf00812192

Title: Login to Disabled Account
- description: Detect failed attempts to sign in to disabled accounts.

- category: data/rules/cloud/azure
- level: medium
- id: 908655e0-25cf-4ae1-b775-1c8ce9cf43d8

Title: Rare Subscription-level Operations In Azure
- description: Identifies IPs from which users grant access to other users on azure resources and alerts when a previously uns
- category: data/rules/cloud/azure
- level: medium
- id: c1182e02-49a3-481c-b3de-0fadc4091488

Title: Google Cloud Firewall Modified or Deleted
- description: Detects when a firewall rule is modified or deleted in Google Cloud Platform (GCP).
- category: data/rules/cloud/gcp
- level: medium
- id: fe513c69-734c-4d4a-8548-ac5f609be82b

Title: Google Cloud Re-identifies Sensitive Information
- description: Identifies when sensitive information is re-identified in google Cloud.
- category: data/rules/cloud/gcp
- level: medium
- id: 234f9f48-904b-4736-a34c-55d23919e4b7

Title: Google Cloud DNS Zone Modified or Deleted
- description: Identifies when a DNS Zone is modified or deleted in Google Cloud.
- category: data/rules/cloud/gcp
- level: medium
- id: 28268a8f-191f-4c17-85b2-f5aa4fa829c3

Title: Google Full Network Traffic Packet Capture
- description: Identifies potential full network packet capture in gcp. This feature can potentially be abused to read sensiti
- category: data/rules/cloud/gcp
- level: medium
- id: 980a7598-1e7f-4962-9372-2d754c930d0e

Title: Google Cloud Storage Buckets Modified or Deleted
- description: Detects when storage bucket is modified or deleted in Google Cloud.
- category: data/rules/cloud/gcp
- level: medium
- id: 4d9f2ee2-c903-48ab-b9c1-8c0f474913d0

Title: Google Cloud Kubernetes Admission Controller
- description: Identifies when an admission controller is executed in GCP Kubernetes. A Kubernetes Admission controller interc
- category: data/rules/cloud/gcp
- level: medium
- id: 6ad91e31-53df-4826-bd27-0166171c8040

Title: Google Cloud SQL Database Modified or Deleted
- description: Detect when a Cloud SQL DB has been modified or deleted.
- category: data/rules/cloud/gcp
- level: medium
- id: f346bbd5-2c4e-4789-a221-72de7685090d

Title: Google Cloud Kubernetes Secrets Modified or Deleted
- description: Identifies when the Secrets are Modified or Deleted.
- category: data/rules/cloud/gcp
- level: medium
- id: 2f0bae2d-bf20-4465-be86-1311addebaa3

Title: Google Cloud Kubernetes CronJob
- description: Identifies when a Google Cloud Kubernetes CronJob runs in Azure Cloud. Kubernetes Job is a controller that crea
- category: data/rules/cloud/gcp
- level: medium
- id: cd3a808c-c7b7-4c50-a2f3-f4cfcd436435

Title: Google Cloud Kubernetes RoleBinding
- description: Detects the creation or patching of potential malicious RoleBinding. This includes RoleBindings and ClusterRole
- category: data/rules/cloud/gcp
- level: medium
- id: 0322d9f2-289a-47c2-b5e1-b63c90901a3e

Title: Google Cloud Service Account Disabled or Deleted
- description: Identifies when a service account is disabled or deleted in Google Cloud.
- category: data/rules/cloud/gcp
- level: medium
- id: 13f81a90-a69c-4fab-8f07-b5bb55416a9f

Title: Google Cloud Service Account Modified
- description: Identifies when a service account is modified in Google Cloud.
- category: data/rules/cloud/gcp
- level: medium
- id: 6b67c12e-5e40-47c6-b3b0-1e6b571184cc

Title: Google Cloud Storage Buckets Enumeration
- description: Detects when storage bucket is enumerated in Google Cloud.
- category: data/rules/cloud/gcp
- level: low
- id: e2feb918-4e77-4608-9697-990a1aaf74c3

Title: Google Cloud VPN Tunnel Modified or Deleted
- description: Identifies when a VPN Tunnel Modified or Deleted in Google Cloud.
- category: data/rules/cloud/gcp
- level: medium
- id: 99980a85-3a61-43d3-ac0f-b68d6b4797b1

Title: AWS Config Disabling Channel/Recorder
- description: Detects AWS Config Service disabling
- category: data/rules/cloud/aws
- level: high
- id: 07330162-dba1-4746-8121-a9647d49d297

Title: AWS IAM Backdoor Users Keys
- description: Detects AWS API key creation for a user by another user. Backdoored users can be used to obtain persistence in
- category: data/rules/cloud/aws
- level: medium
- id: 0a5177f4-6ca9-44c2-aacf-d3f3d8b6e4d2

Title: AWS STS GetSessionToken Misuse
- description: Identifies the suspicious use of GetSessionToken. Tokens could be created and used by attackers to move lateral
- category: data/rules/cloud/aws
- level: low
- id: b45ab1d2-712f-4f01-a751-df3826969807

Title: AWS EC2 Disable EBS Encryption
- description: Identifies disabling of default Amazon Elastic Block Store (EBS) encryption in the current region. Disabling de
- category: data/rules/cloud/aws
- level: medium
- id: 16124c2d-e40b-4fcc-8f2c-5ab7870a2223

Title: AWS STS AssumeRole Misuse
- description: Identifies the suspicious use of AssumeRole. Attackers could move laterally and escalate privileges.
- category: data/rules/cloud/aws
- level: low
- id: 905d389b-b853-46d0-9d3d-dea0d3a3cd49

Title: AWS SecurityHub Findings Evasion
- description: Detects the modification of the findings on SecurityHub.
- category: data/rules/cloud/aws
- level: high
- id: a607e1fe-74bf-4440-a3ec-b059b9103157

Title: Restore Public AWS RDS Instance
- description: Detects the recovery of a new public database instance from a snapshot. It may be a part of data exfiltration.
- category: data/rules/cloud/aws
- level: high
- id: c3f265c7-ff03-4056-8ab2-d486227b4599

Title: AWS EC2 Download Userdata
- description: Detects bulk downloading of User Data associated with AWS EC2 instances. Instance User Data may include install

- category: data/rules/cloud/aws
- level: medium
- id: 26ff4080-194e-47e7-9889-ef7602efed0c

Title: AWS Route 53 Domain Transfer Lock Disabled
- description: Detects when a transfer lock was removed from a Route 53 domain. It is recommended to refrain from performing t
- category: data/rules/cloud/aws
- level: low
- id: 3940b5f1-3f46-44aa-b746-ebe615b879e0

Title: AWS EC2 Startup Shell Script Change
- description: Detects changes to the EC2 instance startup script. The shell script will be executed as root/SYSTEM every time
- category: data/rules/cloud/aws
- level: high
- id: 1ab3c5ed-5baf-417b-bb6b-78ca33f6c3df

Title: AWS EKS Cluster Created or Deleted
- description: Identifies when an EKS cluster is created or deleted.
- category: data/rules/cloud/aws
- level: low
- id: 33d50d03-20ec-4b74-a74e-1e65a38af1c0

Title: AWS Suspicious SAML Activity
- description: Identifies when suspicious SAML activity has occurred in AWS. An adversary could gain backdoor access via SAML.
- category: data/rules/cloud/aws
- level: medium
- id: f43f5d2f-3f2a-4cc8-b1af-81fde7dbaf0e

Title: AWS Macie Evasion
- description: Detects evade to Macie detection.
- category: data/rules/cloud/aws
- level: medium
- id: 91f6a16c-ef71-437a-99ac-0b070e3ad221

Title: AWS Lambda Function Created or Invoked
- description: Detects when an user creates or invokes a lambda function.
- category: data/rules/cloud/aws
- level: low
- id: d914951b-52c8-485f-875e-86abab710c0b

Title: AWS Route 53 Domain Transferred to Another Account
- description: Detects when a request has been made to transfer a Route 53 domain to another AWS account.
- category: data/rules/cloud/aws
- level: low
- id: b056de1a-6e6e-4e40-a67e-97c9808cf41b

Title: AWS Glue Development Endpoint Activity
- description: Detects possible suspicious glue development endpoint activity.
- category: data/rules/cloud/aws
- level: low
- id: 4990c2e3-f4b8-45e3-bc3c-30b14ff0ed26

Title: AWS RDS Master Password Change
- description: Detects the change of database master password. It may be a part of data exfiltration.
- category: data/rules/cloud/aws
- level: medium
- id: 8a63cdd4-6207-414a-85bc-7e032bd3c1a2

Title: AWS GuardDuty Important Change
- description: Detects updates of the GuardDuty list of trusted IPs, perhaps to disable security alerts against malicious IPs.
- category: data/rules/cloud/aws
- level: high
- id: 6e61ee20-ce00-4f8d-8aee-bedd8216f7e3

Title: AWS EC2 VM Export Failure
- description: An attempt to export an AWS EC2 instance has been detected. A VM Export might indicate an attempt to extract in
- category: data/rules/cloud/aws
- level: low
- id: 54b9a76a-3c71-4673-b4b3-2edb4566ea7b

Title: AWS CloudTrail Important Change
- description: Detects disabling, deleting and updating of a Trail
- category: data/rules/cloud/aws
- level: medium
- id: 4db60cc0-36fb-42b7-9b58-a5b53019fb74

Title: AWS Attached Malicious Lambda Layer
- description: Detects when an user attached a Lambda layer to an existing function to override a library that is in use by th
- category: data/rules/cloud/aws
- level: medium
- id: 97fbabf8-8e1b-47a2-b7d5-a418d2b95e3d

Title: AWS Snapshot Backup Exfiltration
- description: Detects the modification of an EC2 snapshot's permissions to enable access from another account
- category: data/rules/cloud/aws
- level: medium
- id: abae8fec-57bd-4f87-aff6-6e3db989843d

Title: AWS Root Credentials
- description: Detects AWS root account usage
- category: data/rules/cloud/aws
- level: medium
- id: 8ad1600d-e9dc-4251-b0ee-a65268f29add

Title: AWS EFS Fileshare Mount Modified or Deleted
- description: Detects when a EFS Fileshare Mount is modified or deleted. An adversary breaking any file system using the moun
- category: data/rules/cloud/aws
- level: medium
- id: 6a7ba45c-63d8-473e-9736-2eaabff79964

Title: AWS ElastiCache Security Group Modified or Deleted
- description: Identifies when an ElastiCache security group has been modified or deleted.
- category: data/rules/cloud/aws
- level: low
- id: 7c797da2-9cf2-4523-ba64-33b06339f0cc

Title: AWS ElastiCache Security Group Created
- description: Detects when an ElastiCache security group has been created.
- category: data/rules/cloud/aws
- level: low
- id: 4ae68615-866f-4304-b24b-ba048dfa5ca7

Title: AWS S3 Data Management Tampering
- description: Detects when a user tampers with S3 data management in Amazon Web Services.
- category: data/rules/cloud/aws
- level: low
- id: 78b3756a-7804-4ef7-8555-7b9024a02e2d

Title: Account Enumeration on AWS
- description: Detects enumeration of accounts configuration via api call to list different instances and services within a sh
- category: data/rules/cloud/aws
- level: low
- id: e9c14b23-47e2-4a8b-8a63-d36618e33d70

Title: AWS User Login Profile Was Modified
- description: An attacker with the iam:UpdateLoginProfile permission on other users can change the password used to login to

With this alert, it is used to detect anyone is changing password on behalf of other users.

- category: data/rules/cloud/aws
- level: high
- id: 055fb148-60f8-462d-ad16-26926ce050f1

Title: AWS EFS Fileshare Modified or Deleted
- description: Detects when a EFS Fileshare is modified or deleted. You can't delete a file system that is in use. If the file
- category: data/rules/cloud/aws
- level: medium
- id: 25cb1ba1-8a19-4a23-a198-d252664c8cef

Title: Google Workspace MFA Disabled
- description: Detects when multi-factor authentication (MFA) is disabled.
- category: data/rules/cloud/gworkspace
- level: medium
- id: 780601d1-6376-4f2a-884e-b8d45599f78c

Title: Google Workspace User Granted Admin Privileges
- description: Detects when an Google Workspace user is granted admin privileges.
- category: data/rules/cloud/gworkspace
- level: medium
- id: 2d1b83e4-17c6-4896-a37b-29140b40a788

Title: Google Workspace Role Privilege Deleted
- description: Detects when an a role privilege is deleted in Google Workspace.
- category: data/rules/cloud/gworkspace
- level: medium
- id: bf638ef7-4d2d-44bb-a1dc-a238252e6267

Title: Google Workspace Application Removed
- description: Detects when an an application is removed from Google Workspace.
- category: data/rules/cloud/gworkspace
- level: medium
- id: ee2803f0-71c8-4831-b48b-a1fc57601ee4

Title: Google Workspace Granted Domain API Access
- description: Detects when an API access service account is granted domain authority.
- category: data/rules/cloud/gworkspace
- level: medium
- id: 04e2a23a-9b29-4a5c-be3a-3542e3f982ba

Title: Google Workspace Role Modified or Deleted
- description: Detects when an a role is modified or deleted in Google Workspace.
- category: data/rules/cloud/gworkspace
- level: medium
- id: 6aef64e3-60c6-4782-8db3-8448759c714e

Title: OneLogin User Assumed Another User
- description: Detects when an user assumed another user account.
- category: data/rules/cloud/onelogin
- level: low
- id: 62fff148-278d-497e-8ecd-ad6083231a35

Title: OneLogin User Account Locked
- description: Detects when an user acount is locked or suspended.
- category: data/rules/cloud/onelogin
- level: low
- id: a717c561-d117-437e-b2d9-0118a7035d01

Title: Raw Disk Access Using Illegitimate Tools
- description: Raw disk access using illegitimate tools, possible defence evasion
- category: data/rules/windows/raw_access_thread
- level: low
- id: db809f10-56ce-4420-8c86-d6a7d793c79c

Title: Delete Log from Application
- description: Deletion of log files is a known anti-forensic technique
- category: data/rules/windows/file_delete
- level: low
- id: b1decb61-ed83-4339-8e95-53ea51901720

Title: Deletes Backup Files
- description: Adversaries may delete or remove built-in operating system data and turn off services designed to aid in the re
- category: data/rules/windows/file_delete
- level: medium
- id: 06125661-3814-4e03-bfa2-1e4411c60ac3

Title: Windows Spooler Service Suspicious File Deletion
- description: Detect DLL deletions from Spooler Service driver folder

- category: data/rules/windows/file_delete
- level: high
- id: 5b2bbc47-dead-4ef7-8908-0cf73fcbecbf

Title: Sysinternals SDelete File Deletion
- description: A General detection to trigger for the deletion of files by Sysinternals SDelete. It looks for the common name
- category: data/rules/windows/file_delete
- level: medium
- id: 6ddab845-b1b8-49c2-bbf7-1a11967f64bc

Title: Prefetch File Deletion
- description: Detects the deletion of a prefetch file (AntiForensic)
- category: data/rules/windows/file_delete
- level: high
- id: 0a1f9d29-6465-4776-b091-7f43b26e4c89

Title: Suspicious Scripting in a WMI Consumer
- description: Detects suspicious scripting in WMI Event Consumers
- category: data/rules/windows/wmi_event
- level: high
- id: fe21810c-2a8c-478f-8dd3-5a287fb2a0e0

Title: Suspicious Encoded Scripts in a WMI Consumer
- description: Detects suspicious encoded payloads in WMI Event Consumers
- category: data/rules/windows/wmi_event
- level: high
- id: 83844185-1c5b-45bc-bcf3-b5bf3084ca5b

Title: WMI Event Subscription
- description: Detects creation of WMI event subscription persistence method
- category: data/rules/windows/wmi_event
- level: high
- id: 0f06a3a5-6a09-413f-8743-e6cf35561297

Title: Possible DNS Rebinding
- description: Detects several different DNS-answers by one domain with IPs from internal and external networks. Normally, DNS
- category: data/rules/windows/dns_query
- level: medium
- id: eb07e747-2552-44cd-af36-b659ae0958e4

Title: AppInstaller Attempts From URL by DNS
- description: AppInstaller.exe is spawned by the default handler for the URI, it attempts to load/install a package from the
- category: data/rules/windows/dns_query
- level: medium
- id: 7cff77e1-9663-46a3-8260-17f2e1aa9d0a

Title: Suspicious DNS Query for IP Lookup Service APIs
- description: Detects DNS queries for ip lookup services such as api.ipify.org not originating from a browser process.
- category: data/rules/windows/dns_query
- level: medium
- id: ec82e2a5-81ea-4211-a1f8-37a0286df2c2

Title: Suspicious TeamViewer Domain Access
- description: Detects DNS queries to a TeamViewer domain only resolved by a TeamViewer client by an image that isn't named Te
- category: data/rules/windows/dns_query
- level: medium
- id: 778ba9a8-45e4-4b80-8e3e-34a419f0b85e

Title: Query to Ammyy Remote Access Software Domain
- description: An adversary may use legitimate desktop support and remote access software, such as Team Viewer, Go2Assist, Log

These services are commonly used as legitimate technical support software, and may be allowed by application control within a target environment. Remote access tools like VNC, Ammyy, and Teamviewer are used frequently when compared with other legitimate software commonly used by adversaries. (Citation: Symantec Living off the Land)

- category: data/rules/windows/dns_query
- level: medium
- id: 71ba22cb-8a01-42e2-a6dd-5bf9b547498f

```
Title: DNS Query for MEGA.io Upload Domain
- description: Detects DNS queries for subdomains used for upload to MEGA.io
- category: data/rules/windows/dns_query
- level: high
- id: 613c03ba-0779-4a53-8a1f-47f914a4ded3

Title: Regsvr32 Network Activity
- description: Detects network connections and DNS queries initiated by Regsvr32.exe
- category: data/rules/windows/dns_query
- level: high
- id: 36e037c4-c228-4866-b6a3-48eb292b9955

Title: Query to LogMeIn Remote Access Software Domain
- description: An adversary may use legitimate desktop support and remote access software, such as Team Viewer, Go2Assist, Log
```

These services are commonly used as legitimate technical support software, and may be allowed by application control within a target environment. Remote access tools like VNC, Ammyy, and Teamviewer are used frequently when compared with other legitimate software commonly used by adversaries. (Citation: Symantec Living off the Land)

```
- category: data/rules/windows/dns_query
- level: medium
- id: ed785237-70fa-46f3-83b6-d264d1dc6eb4

Title: Query to GoToAssist Remote Access Software Domain
- description: An adversary may use legitimate desktop support and remote access software, such as Team Viewer, Go2Assist, Log
```

These services are commonly used as legitimate technical support software, and may be allowed by application control within a target environment. Remote access tools like VNC, Ammyy, and Teamviewer are used frequently when compared with other legitimate software commonly used by adversaries. (Citation: Symantec Living off the Land)

```
- category: data/rules/windows/dns_query
- level: medium
- id: 7c4cf8e0-1362-48b2-a512-b606d2065d7d

Title: Query Tor Onion Address
- description: Detects DNS resolution of an .onion address related to Tor routing networks
- category: data/rules/windows/dns_query
- level: high
- id: b55ca2a3-7cff-4dda-8bdd-c7bfa63bf544

Title: Suspicious Cobalt Strike DNS Beaconing
- description: Detects a program that invoked suspicious DNS queries known from Cobalt Strike beacons
- category: data/rules/windows/dns_query
- level: critical
- id: f356a9c4-effd-4608-bbf8-408afd5cd006

Title: DNS HybridConnectionManager Service Bus
- description: Detects Azure Hybrid Connection Manager services querying the Azure service bus service
- category: data/rules/windows/dns_query
- level: high
- id: 7bd3902d-8b8b-4dd4-838a-c6862d40150d

Title: Suspicious Driver Install by pnputil.exe
- description: Detects when a possible suspicious driver is being installed via pnputil.exe lolbin
- category: data/rules/windows/process_creation
- level: medium
- id: a2ea3ae7-d3d0-40a0-a55c-25a45c87cac1

Title: Regsvr32 Flags Anomaly
- description: Detects a flag anomaly in which regsvr32.exe uses a /i flag without using a /n flag at the same time
- category: data/rules/windows/process_creation
- level: high
- id: b236190c-1c61-41e9-84b3-3fe03f6d76b0

Title: Code Execution via Pcwutl.dll
- description: Detects launch of executable by calling the LaunchApplication function from pcwutl.dll library.
- category: data/rules/windows/process_creation
- level: medium
- id: 9386d78a-7207-4048-9c9f-a93a7c2d1c05
```

Title: Curl Start Combination
- description: Adversaries can use curl to download payloads remotely and execute them. Curl is included by default in Windows
- category: data/rules/windows/process_creation
- level: medium
- id: 21dd6d38-2b18-4453-9404-a0fe4a0cc288

Title: Mustang Panda Dropper
- description: Detects specific process parameters as used by Mustang Panda droppers
- category: data/rules/windows/process_creation
- level: high
- id: 2d87d610-d760-45ee-a7e6-7a6f2a65de00

Title: Turla Group Commands May 2020
- description: Detects commands used by Turla group as reported by ESET in May 2020
- category: data/rules/windows/process_creation
- level: critical
- id: 9e2e51c5-c699-4794-ba5a-29f5da40ac0c

Title: Suspicious TSCON Start as SYSTEM
- description: Detects a tscon.exe start as LOCAL SYSTEM
- category: data/rules/windows/process_creation
- level: high
- id: 9847f263-4a81-424f-970c-875dab15b79b

Title: File or Folder Permissions Modifications
- description: Detects a file or folder's permissions being modified.
- category: data/rules/windows/process_creation
- level: medium
- id: 37ae075c-271b-459b-8d7b-55ad5f993dd8

Title: Detecting Fake Instances Of Hxtsr.exe
- description: HxTsr.exe is a Microsoft compressed executable file called Microsoft Outlook Communications.HxTsr.exe is part o
- category: data/rules/windows/process_creation
- level: medium
- id: 4e762605-34a8-406d-b72e-c1a089313320

Title: Explorer Root Flag Process Tree Break
- description: Detects a command line process that uses explorer.exe /root, which is similar to cmd.exe /c, only it breaks the
- category: data/rules/windows/process_creation
- level: medium
- id: 949f1ffb-6e85-4f00-ae1e-c3c5b190d605

Title: Procdump Evasion
- description: Detects uses of the SysInternals Procdump utility in which procdump or its output get renamed or a dump file is
- category: data/rules/windows/process_creation
- level: high
- id: 79b06761-465f-4f88-9ef2-150e24d3d737

Title: Powershell Defender Exclusion
- description: Detects requests to exclude files, folders or processes from Antivirus scanning using PowerShell cmdlets
- category: data/rules/windows/process_creation
- level: medium
- id: 17769c90-230e-488b-a463-e05c08e9d48f

Title: Rclone Execution via Command Line or PowerShell
- description: Detects execution of RClone utility for exfiltration as used by various ransomwares strains like REvil, Conti,
- category: data/rules/windows/process_creation
- level: high
- id: e37db05d-d1f9-49c8-b464-cee1a4b11638

Title: Suspicious Extrac32 Alternate Data Stream Execution
- description: Extract data from cab file and hide it in an alternate data stream
- category: data/rules/windows/process_creation
- level: medium
- id: 4b13db67-0c45-40f1-aba8-66a1a7198a1e

Title: Suspicious Control Panel DLL Load
- description: Detects suspicious Rundll32 execution from control.exe as used by Equation Group and Exploit Kits
- category: data/rules/windows/process_creation

- level: high
- id: d7eb979b-c2b5-4a6f-a3a7-c87ce6763819

Title: Rar Usage with Password and Compression Level
- description: Detects the use of rar.exe, on the command line, to create an archive with password protection or with a specif
- category: data/rules/windows/process_creation
- level: high
- id: faa48cae-6b25-4f00-a094-08947fef582f

Title: Data Compressed - rar.exe
- description: An adversary may compress data (e.g., sensitive documents) that is collected prior to exfiltration in order to
- category: data/rules/windows/process_creation
- level: low
- id: 6f3e2987-db24-4c78-a860-b4f4095a7095

Title: Suspicious Network Command
- description: Adversaries may look for details about the network configuration and settings of systems they access or through
- category: data/rules/windows/process_creation
- level: low
- id: a29c1813-ab1f-4dde-b489-330b952e91ae

Title: WhoAmI as Parameter
- description: Detects a suspicious process command line that uses whoami as first parameter (as e.g. used by EfsPotato)
- category: data/rules/windows/process_creation
- level: high
- id: e9142d84-fbe0-401d-ac50-3e519fb00c89

Title: DLL Execution via Rasautou.exe
- description: Detects using Rasautou.exe for loading arbitrary .DLL specified in -d option and executes the export specified
- category: data/rules/windows/process_creation
- level: medium
- id: cd3d1298-eb3b-476c-ac67-12847de55813

Title: Suspicious WMIC ActiveScriptEventConsumer Creation
- description: Detects WMIC executions in which a event consumer gets created in order to establish persistence
- category: data/rules/windows/process_creation
- level: high
- id: ebef4391-1a81-4761-a40a-1db446c0e625

Title: Suspicious Sc Query
- description: Adversaries may try to get information about registered services
- category: data/rules/windows/process_creation
- level: low
- id: 57712d7a-679c-4a41-a913-87e7175ae429

Title: Execute Code with Pester.bat
- description: Detects code execution via Pester.bat (Pester - Powershell Modulte for testing)
- category: data/rules/windows/process_creation
- level: medium
- id: 59e938ff-0d6d-4dc3-b13f-36cc28734d4e

Title: Renamed SysInternals Debug View
- description: Detects suspicious renamed SysInternals DebugView execution
- category: data/rules/windows/process_creation
- level: high
- id: cd764533-2e07-40d6-a718-cfeec7f2da7f

Title: Lazarus Activity
- description: Detects different process creation events as described in Malwarebytes's threat report on Lazarus group activit
- category: data/rules/windows/process_creation
- level: critical
- id: 4a12fa47-c735-4032-a214-6fab5b120670

Title: Suspicious Userinit Child Process
- description: Detects a suspicious child process of userinit
- category: data/rules/windows/process_creation
- level: medium
- id: b655a06a-31c0-477a-95c2-3726b83d649d

Title: Ilasm Lolbin Use Compile C-Sharp
- description: Detect use of Ilasm.exe to compile c# code into dll or exe.
- category: data/rules/windows/process_creation
- level: medium
- id: 850d55f9-6eeb-4492-ad69-a72338f65ba4

Title: MSTSC Shadowing
- description: Detects RDP session hijacking by using MSTSC shadowing
- category: data/rules/windows/process_creation
- level: high
- id: 6ba5a05f-b095-4f0a-8654-b825f4f16334

Title: Execution via WorkFolders.exe
- description: Detects using WorkFolders.exe to execute an arbitrary control.exe
- category: data/rules/windows/process_creation
- level: high
- id: 0bbc6369-43e3-453d-9944-cae58821c173

Title: CrackMapExecWin
- description: Detects CrackMapExecWin Activity as Described by NCSC
- category: data/rules/windows/process_creation
- level: critical
- id: 04d9079e-3905-4b70-ad37-6bdf11304965

Title: LockerGoga Ransomware
- description: Detects LockerGoga Ransomware command line.
- category: data/rules/windows/process_creation
- level: critical
- id: 74db3488-fd28-480a-95aa-b7af626de068

Title: Overwrite Deleted Data with Cipher
- description: Adversaries may destroy data and files on specific systems or in large numbers on a network to interrupt availa

Data destruction is likely to render stored data irrecoverable by forensic techniques through overwriting files or data on local and remote drives

- category: data/rules/windows/process_creation
- level: medium
- id: 4b046706-5789-4673-b111-66f25fe99534

Title: Replace.exe Usage
- description: Detects the use of Replace.exe which can be used to replace file with another file
- category: data/rules/windows/process_creation
- level: medium
- id: 9292293b-8496-4715-9db6-37028dcda4b3

Title: Possible InstallerFileTakeOver LPE CVE-2021-41379
- description: Detects signs of the exploitation of LPE CVE-2021-41379 to spawn a cmd.exe with LOCAL_SYSTEM rights
- category: data/rules/windows/process_creation
- level: critical
- id: af8bbce4-f751-46b4-8d91-82a33a736f61

Title: Netsh Program Allowed with Suspcious Location
- description: Detects Netsh commands that allows a suspcious application location on Windows Firewall
- category: data/rules/windows/process_creation
- level: high
- id: a35f5a72-f347-4e36-8895-9869b0d5fc6d

Title: Suspicious Execution of InstallUtil Without Log
- description: Uses the .NET InstallUtil.exe application in order to execute image without log
- category: data/rules/windows/process_creation
- level: medium
- id: d042284c-a296-4988-9be5-f424fadcc28c

Title: Hacktool by Cube0x0
- description: Detects the use of tools created by a well-known hacktool producer named Cube0x0, which includes his handle in
- category: data/rules/windows/process_creation
- level: high
- id: 37c1333a-a0db-48be-b64b-7393b2386e3b

Title: Suspicious Desktopimgdownldr Command
- description: Detects a suspicious Microsoft desktopimgdownldr execution with parameters used to download files from the Inte
- category: data/rules/windows/process_creation
- level: high
- id: bb58aa4a-b80b-415a-a2c0-2f65a4c81009

Title: Suspicious SYSTEM User Process Creation
- description: Detects a suspicious process creation as SYSTEM user (suspicious program or command line parameter)
- category: data/rules/windows/process_creation
- level: high
- id: 2617e7ed-adb7-40ba-b0f3-8f9945fe6c09

Title: Shadow Copies Deletion Using Operating Systems Utilities
- description: Shadow Copies deletion using operating systems utilities
- category: data/rules/windows/process_creation
- level: critical
- id: c947b146-0abc-4c87-9c64-b17e9d7274a2

Title: Scheduled Task Creation
- description: Detects the creation of scheduled tasks in user session
- category: data/rules/windows/process_creation
- level: low
- id: 92626ddd-662c-49e3-ac59-f6535f12d189

Title: CVE-2021-40444 Process Pattern
- description: Detects a suspicious process pattern found in CVE-2021-40444 exploitation
- category: data/rules/windows/process_creation
- level: critical
- id: 894397c6-da03-425c-a589-3d09e7d1f750

Title: SyncAppvPublishingServer Execute Arbitrary PowerShell Code
- description: Executes arbitrary PowerShell code using SyncAppvPublishingServer.exe.
- category: data/rules/windows/process_creation
- level: medium
- id: fbd7c32d-db2a-4418-b92c-566eb8911133

Title: Exploit for CVE-2015-1641
- description: Detects Winword starting uncommon sub process MicroScMgmt.exe as used in exploits for CVE-2015-1641
- category: data/rules/windows/process_creation
- level: critical
- id: 7993792c-5ce2-4475-a3db-a3a5539827ef

Title: Service Execution
- description: Detects manual service execution (start) via system utilities.
- category: data/rules/windows/process_creation
- level: low
- id: 2a072a96-a086-49fa-bcb5-15cc5a619093

Title: Suspicious Curl Change User Agents
- description: Detects a suspicious curl process start on Windows with set useragent options
- category: data/rules/windows/process_creation
- level: medium
- id: 3286d37a-00fd-41c2-a624-a672dcd34e60

Title: FromBase64String Command Line
- description: Detects suspicious FromBase64String expressions in command line arguments
- category: data/rules/windows/process_creation
- level: high
- id: e32d4572-9826-4738-b651-95fa63747e8a

Title: System File Execution Location Anomaly
- description: Detects a Windows program executable started in a suspicious folder
- category: data/rules/windows/process_creation
- level: high
- id: e4a6b256-3e47-40fc-89d2-7a477edd6915

Title: Possible Privilege Escalation via Service Permissions Weakness
- description: Detect modification of services configuration (ImagePath, FailureCommand and ServiceDLL) in registry by process
- category: data/rules/windows/process_creation

- level: high
- id: 0f9c21f1-6a73-4b0e-9809-cb562cb8d981

Title: Sticky-Key Backdoor Copy Cmd.exe
- description: By replacing the sticky keys executable with the local admins CMD executable, an attacker is able to access a p
- category: data/rules/windows/process_creation
- level: medium
- id: 1070db9a-3e5d-412e-8e7b-7183b616e1b3

Title: CHCP CodePage Locale Lookup
- description: Detects use of chcp to look up the system locale value as part of host discovery
- category: data/rules/windows/process_creation
- level: high
- id: 7090adee-82e2-4269-bd59-80691e7c6338

Title: Windows Crypto Mining Indicators
- description: Detects command line parameters or strings often used by crypto miners
- category: data/rules/windows/process_creation
- level: high
- id: 66c3b204-9f88-4d0a-a7f7-8a57d521ca55

Title: Baby Shark Activity
- description: Detects activity that could be related to Baby Shark malware
- category: data/rules/windows/process_creation
- level: high
- id: 2b30fa36-3a18-402f-a22d-bf4ce2189f35

Title: Execution Of Non-Existing File
- description: Checks whether the image specified in a process creation event is not a full, absolute path (caused by process
- category: data/rules/windows/process_creation
- level: high
- id: 71158e3f-df67-472b-930e-7d287acaa3e1

Title: Netsh Allow Group Policy on Microsoft Defender Firewall
- description: Adversaries may modify system firewalls in order to bypass controls limiting network usage
- category: data/rules/windows/process_creation
- level: medium
- id: 347906f3-e207-4d18-ae5b-a9403d6bcdef

Title: XSL Script Processing
- description: Extensible Stylesheet Language (XSL) files are commonly used to describe the processing and rendering of data w
- category: data/rules/windows/process_creation
- level: medium
- id: 05c36dd6-79d6-4a9a-97da-3db20298ab2d

Title: Advanced IP Scanner
- description: Detects the use of Advanced IP Scanner. Seems to be a popular tool for ransomware groups.
- category: data/rules/windows/process_creation
- level: medium
- id: bef37fa2-f205-4a7b-b484-0759bfd5f86f

Title: UAC Bypass Using Windows Media Player - Process
- description: Detects the pattern of UAC Bypass using Windows Media Player osksupport.dll (UACMe 32)
- category: data/rules/windows/process_creation
- level: high
- id: 0058b9e5-bcd7-40d4-9205-95ca5a16d7b2

Title: Modifies the Registry From a ADS
- description: Detects the import of an alternate data stream with regini.exe, regini.exe can be used to modify registry keys.
- category: data/rules/windows/process_creation
- level: high
- id: 77946e79-97f1-45a2-84b4-f37b5c0d8682

Title: Suspicious Service Path Modification
- description: Detects service path modification to PowerShell or cmd.
- category: data/rules/windows/process_creation
- level: high
- id: 138d3531-8793-4f50-a2cd-f291b2863d78

Title: Run PowerShell Script from ADS
- description: Detects PowerShell script execution from Alternate Data Stream (ADS)
- category: data/rules/windows/process_creation
- level: high
- id: 45a594aa-1fbd-4972-a809-ff5a99dd81b8

Title: Ke3chang Registry Key Modifications
- description: Detects Registry modifications performed by Ke3chang malware in campaigns running in 2019 and 2020
- category: data/rules/windows/process_creation
- level: critical
- id: 7b544661-69fc-419f-9a59-82ccc328f205

Title: Suspicious Bitsadmin Job via PowerShell
- description: Detect download by BITS jobs via PowerShell
- category: data/rules/windows/process_creation
- level: high
- id: f67dbfce-93bc-440d-86ad-a95ae8858c90

Title: RunXCmd Tool Execution As System
- description: Detects the use of RunXCmd tool for command execution
- category: data/rules/windows/process_creation
- level: high
- id: 93199800-b52a-4dec-b762-75212c196542

Title: Malicious PE Execution by Microsoft Visual Studio Debugger
- description: There is an option for a MS VS Just-In-Time Debugger "vsjitdebugger.exe" to launch specified executable and att
- category: data/rules/windows/process_creation
- level: medium
- id: 15c7904e-6ad1-4a45-9b46-5fb25df37fd2

Title: PowerShell Downgrade Attack
- description: Detects PowerShell downgrade attack by comparing the host versions with the actually used engine version 2.0
- category: data/rules/windows/process_creation
- level: medium
- id: b3512211-c67e-4707-bedc-66efc7848863

Title: Conhost Parent Process Executions
- description: Detects the conhost execution as parent process. Can be used to evaded defense mechanism.
- category: data/rules/windows/process_creation
- level: medium
- id: 7dc2dedd-7603-461a-bc13-15803d132355

Title: Copying Sensitive Files with Credential Data
- description: Files with well-known filenames (sensitive files with credential data) copying
- category: data/rules/windows/process_creation
- level: high
- id: e7be6119-fc37-43f0-ad4f-1f3f99be2f9f

Title: Highly Relevant Renamed Binary
- description: Detects the execution of a renamed binary often used by attackers or malware leveraging new Sysmon OriginalFile
- category: data/rules/windows/process_creation
- level: high
- id: 0ba1da6d-b6ce-4366-828c-18826c9de23e

Title: Serv-U Exploitation CVE-2021-35211 by DEV-0322
- description: Detects patterns as noticed in exploitation of Serv-U CVE-2021-35211 vulnerability by threat group DEV-0322
- category: data/rules/windows/process_creation
- level: critical
- id: 75578840-9526-4b2a-9462-af469a45e767

Title: Suspicious Netsh Discovery Command
- description: Adversaries may look for details about the network configuration and settings of systems they access or through
- category: data/rules/windows/process_creation
- level: low
- id: 0e4164da-94bc-450d-a7be-a4b176179f1f

Title: TropicTrooper Campaign November 2018
- description: Detects TropicTrooper activity, an actor who targeted high-profile organizations in the energy and food and bev
- category: data/rules/windows/process_creation

- level: high
- id: 8c7090c3-e0a0-4944-bd08-08c3a0cecf79

Title: CMSTP Execution Process Creation
- description: Detects various indicators of Microsoft Connection Manager Profile Installer execution
- category: data/rules/windows/process_creation
- level: high
- id: 7d4cdc5a-0076-40ca-aac8-f7e714570e47

Title: Suspicious Extrac32 Execution
- description: Download or Copy file with Extrac32
- category: data/rules/windows/process_creation
- level: medium
- id: aa8e035d-7be4-48d3-a944-102aec04400d

Title: Suspicious LOLBIN AccCheckConsole
- description: Detects suspicious LOLBIN AccCheckConsole execution with parameters as used to load an arbitrary DLL
- category: data/rules/windows/process_creation
- level: high
- id: 0f6da907-5854-4be6-859a-e9958747b0aa

Title: Capture a Network Trace with netsh.exe
- description: Detects capture a network trace via netsh.exe trace functionality
- category: data/rules/windows/process_creation
- level: medium
- id: d3c3861d-c504-4c77-ba55-224ba82d0118

Title: Quick Execution of a Series of Suspicious Commands
- description: Detects multiple suspicious process in a limited timeframe
- category: data/rules/windows/process_creation
- level: low
- id: 61ab5496-748e-4818-a92f-de78e20fe7f1

Title: Windows Credential Manager Access via VaultCmd
- description: List credentials currently stored in Windows Credential Manager via the native Windows utility vaultcmd.exe
- category: data/rules/windows/process_creation
- level: medium
- id: 58f50261-c53b-4c88-bd12-1d71f12eda4c

Title: REvil Kaseya Incident Malware Patterns
- description: Detects process command line patterns and locations used by REvil group in Kaseya incident (can also match on o
- category: data/rules/windows/process_creation
- level: critical
- id: 5de632bc-7fbd-4c8a-944a-fce55c59eae5

Title: Rundll32 From Abnormal Drive
- description: Detects rundll32.exe executing from an abnormal drive such as a mounted ISO.
- category: data/rules/windows/process_creation
- level: medium
- id: d4ca7c59-e9e4-42d8-bf57-91a776efcb87

Title: PsExec/PAExec Flags
- description: Detects suspicious flags used by PsExec and PAExec but no usual program name in command line
- category: data/rules/windows/process_creation
- level: high
- id: 207b0396-3689-42d9-8399-4222658efc99

Title: Turla Group Lateral Movement
- description: Detects automated lateral movement by Turla group
- category: data/rules/windows/process_creation
- level: medium
- id: 75925535-ca97-4e0a-a850-00b5c00779dc

Title: Hurricane Panda Activity
- description: Detects Hurricane Panda Activity
- category: data/rules/windows/process_creation
- level: high
- id: 0eb2107b-a596-422e-b123-b389d5594ed7

Title: Suspicious PowerShell Sub Processes
- description: Detects suspicious sub processes spawned by PowerShell
- category: data/rules/windows/process_creation
- level: high
- id: e4b6d2a7-d8a4-4f19-acbd-943c16d90647

Title: Suspicious Calculator Usage
- description: Detects suspicious use of calc.exe with command line parameters or in a suspicious directory, which is likely c
- category: data/rules/windows/process_creation
- level: high
- id: 737e618a-a410-49b5-bec3-9e55ff7fbc15

Title: Execute From Alternate Data Streams
- description: Adversaries may use NTFS file attributes to hide their malicious data in order to evade detection
- category: data/rules/windows/process_creation
- level: medium
- id: 7f43c430-5001-4f8b-aaa9-c3b88f18fa5c

Title: NirCmd Tool Execution As LOCAL SYSTEM
- description: Detects the use of NirCmd tool for command execution as SYSTEM user
- category: data/rules/windows/process_creation
- level: high
- id: d9047477-0359-48c9-b8c7-792cedcdc9c4

Title: Registry Defender Exclusions
- description: Qbot used reg.exe to add Defender folder exceptions for folders within AppData and ProgramData.
- category: data/rules/windows/process_creation
- level: medium
- id: 48917adc-a28e-4f5d-b729-11e75da8941f

Title: Possible Ransomware or Unauthorized MBR Modifications
- description: Detects, possibly, malicious unauthorized usage of bcdedit.exe
- category: data/rules/windows/process_creation
- level: medium
- id: c9fbe8e9-119d-40a6-9b59-dd58a5d84429

Title: Suspicious HWP Sub Processes
- description: Detects suspicious Hangul Word Processor (Hanword) sub processes that could indicate an exploitation
- category: data/rules/windows/process_creation
- level: high
- id: 023394c4-29d5-46ab-92b8-6a534c6f447b

Title: Snatch Ransomware
- description: Detects specific process characteristics of Snatch ransomware word document droppers
- category: data/rules/windows/process_creation
- level: critical
- id: 5325945e-f1f0-406e-97b8-65104d393fff

Title: Windows Suspicious Use Of Web Request in CommandLine
- description: Detects the use of various web request with commandline tools or Windows PowerShell command,methods (including
- category: data/rules/windows/process_creation
- level: medium
- id: 9fc51a3c-81b3-4fa7-b35f-7c02cf10fd2d

Title: Java Running with Remote Debugging
- description: Detects a JAVA process running with remote debugging allowing more than just localhost to connect
- category: data/rules/windows/process_creation
- level: medium
- id: 8f88e3f6-2a49-48f5-a5c4-2f7eedf78710

Title: CleanWipe Usage
- description: Detects the use of CleanWipe a tool usually used to delete Symantec test.
- category: data/rules/windows/process_creation
- level: medium
- id: f44800ac-38ec-471f-936e-3fa7d9c53100

Title: Executable Used by PlugX in Uncommon Location
- description: Detects the execution of an executable that is typically used by PlugX for DLL side loading started from an unc
- category: data/rules/windows/process_creation

- level: high
- id: aeab5ec5-be14-471a-80e8-e344418305c2

Title: Unidentified Attacker November 2018
- description: A sigma rule detecting an unidetefied attacker who used phishing emails to target high profile orgs on November
- category: data/rules/windows/process_creation
- level: high
- id: 7453575c-a747-40b9-839b-125a0aae324b

Title: Suspicious AdvancedRun Runas Priv User
- description: Detects the execution of AdvancedRun utitlity in the context of the TrustedInstaller, SYSTEM, Local Service or
- category: data/rules/windows/process_creation
- level: high
- id: fa00b701-44c6-4679-994d-5a18afa8a707

Title: Discover Private Keys
- description: Adversaries may search for private key certificate files on compromised systems for insecurely stored credentia
- category: data/rules/windows/process_creation
- level: medium
- id: 213d6a77-3d55-4ce8-ba74-fcfef741974e

Title: Run PowerShell Script from Redirected Input Stream
- description: Detects PowerShell script execution via input stream redirect
- category: data/rules/windows/process_creation
- level: high
- id: c83bf4b5-cdf0-437c-90fa-43d734f7c476

Title: Suspicious Call by Ordinal
- description: Detects suspicious calls of DLLs in rundll32.dll exports by ordinal
- category: data/rules/windows/process_creation
- level: high
- id: e79a9e79-eb72-4e78-a628-0e7e8f59e89c

Title: Emissary Panda Malware SLLauncher
- description: Detects the execution of DLL side-loading malware used by threat group Emissary Panda aka APT27
- category: data/rules/windows/process_creation
- level: critical
- id: 9aa01d62-7667-4d3b-acb8-8cb5103e2014

Title: WMI Reconnaissance List Remote Services
- description: An adversary might use WMI to check if a certain Remote Service is running on a remote device.

When the test completes, a service information will be displayed on the screen if it exists. A common feedback message is that "No instance(s) Available" if the service queried is not running. A common error message is "Node - (provided IP or default) ERROR Description =The RPC server is unavailable" if the provided remote host is unreacheable

- category: data/rules/windows/process_creation
- level: medium
- id: 09af397b-c5eb-4811-b2bb-08b3de464ebf

Title: Script Interpreter Execution From Suspicious Folder
- description: Detects a suspicious script executions in temporary folders or folders accessible by environment variables
- category: data/rules/windows/process_creation
- level: high
- id: 1228c958-e64e-4e71-92ad-7d429f4138ba

Title: Suspicious AdFind Execution
- description: Detects the execution of a AdFind for Active Directory enumeration
- category: data/rules/windows/process_creation
- level: medium
- id: 75df3b17-8bcc-4565-b89b-c9898acef911

Title: Suspicious Csc.exe Source File Folder
- description: Detects a suspicious execution of csc.exe, which uses a source in a suspicious folder (e.g. AppData)
- category: data/rules/windows/process_creation
- level: medium
- id: dcaa3f04-70c3-427a-80b4-b870d73c94c4

Title: Suspicious Add Scheduled Task Parent

- description: Detects suspicious scheduled task creations from a parent stored in a temporary folder
- category: data/rules/windows/process_creation
- level: medium
- id: 9494479d-d994-40bf-a8b1-eea890237021

Title: Suspicius Schtasks From Env Var Folder
- description: Detects Schtask creations that point to a folder references in environment variables or often used by malware
- category: data/rules/windows/process_creation
- level: high
- id: 81325ce1-be01-4250-944f-b4789644556f

Title: WSL Execution
- description: Detects Possible usage of Windows Subsystem for Linux (WSL) binary as a LOLBIN
- category: data/rules/windows/process_creation
- level: medium
- id: dec44ca7-61ad-493c-bfd7-8819c5faa09b

Title: CVE-2021-26857 Exchange Exploitation
- description: Detects possible successful exploitation for vulnerability described in CVE-2021-26857 by looking for | abnorma
- category: data/rules/windows/process_creation
- level: critical
- id: cd479ccc-d8f0-4c66-ba7d-e06286f3f887

Title: MSExchange Transport Agent Installation
- description: Detects the Installation of a Exchange Transport Agent
- category: data/rules/windows/process_creation
- level: medium
- id: 83809e84-4475-4b69-bc3e-4aad8568612f

Title: Suspicious Svchost Process
- description: Detects a suspicious svchost process start
- category: data/rules/windows/process_creation
- level: high
- id: 01d2e2a1-5f09-44f7-9fc1-24faa7479b6d

Title: Suspicious Encoded PowerShell Command Line
- description: Detects suspicious powershell process starts with base64 encoded commands (e.g. Emotet)
- category: data/rules/windows/process_creation
- level: high
- id: ca2092a1-c273-4878-9b4b-0d60115bf5ea

Title: Suspicious PowerShell Cmdline
- description: Detects the PowerShell command lines with reversed strings
- category: data/rules/windows/process_creation
- level: high
- id: b6b49cd1-34d6-4ead-b1bf-176e9edba9a4

Title: Ncat Execution
- description: Adversaries may use a non-application layer protocol for communication between host and C2 server or among infe
- category: data/rules/windows/process_creation
- level: high
- id: e31033fc-33f0-4020-9a16-faf9b31cbf08

Title: Explorer NOUACCHECK Flag
- description: Detects suspicious starts of explorer.exe that use the /NOUACCHECK flag that allows to run all sub processes of
- category: data/rules/windows/process_creation
- level: high
- id: 534f2ef7-e8a2-4433-816d-c91bccde289b

Title: COMPlus_ETWEnabled Command Line Arguments
- description: Potential adversaries stopping ETW providers recording loaded .NET assemblies.
- category: data/rules/windows/process_creation
- level: critical
- id: 41421f44-58f9-455d-838a-c398859841d4

Title: InfDefaultInstall.exe .inf Execution
- description: Executes SCT script using scrobj.dll from a command in entered into a specially prepared INF file.
- category: data/rules/windows/process_creation
- level: medium

- id: ce7cf472-6fcc-490a-9481-3786840b5d9b

Title: Imports Registry Key From an ADS
- description: Detects the import of a alternate datastream to the registry with regedit.exe.
- category: data/rules/windows/process_creation
- level: high
- id: 0b80ade5-6997-4b1d-99a1-71701778ea61

Title: ZOHO Dctask64 Process Injection
- description: Detects suspicious process injection using ZOHO's dctask64.exe
- category: data/rules/windows/process_creation
- level: high
- id: 6345b048-8441-43a7-9bed-541133633d7a

Title: Tasks Folder Evasion
- description: The Tasks folder in system32 and syswow64 are globally writable paths. Adversaries can take advantage of this a
- category: data/rules/windows/process_creation
- level: high
- id: cc4e02ba-9c06-48e2-b09e-2500cace9ae0

Title: Office Applications Spawning Wmi Cli
- description: Initial execution of malicious document calls wmic to execute the file with regsvr32
- category: data/rules/windows/process_creation
- level: high
- id: 04f5363a-6bca-42ff-be70-0d28bf629ead

Title: WinRM Access with Evil-WinRM
- description: Adversaries may use Valid Accounts to log into a computer using the Remote Desktop Protocol (RDP). The adversar
- category: data/rules/windows/process_creation
- level: medium
- id: a197e378-d31b-41c0-9635-cfdf1c1bb423

Title: Run Whoami Showing Privileges
- description: Detects a whoami.exe executed with the /priv command line flag instructing the tool to show all current user pr
- category: data/rules/windows/process_creation
- level: high
- id: 97a80ec7-0e2f-4d05-9ef4-65760e634f6b

Title: Meterpreter or Cobalt Strike Getsystem Service Start
- description: Detects the use of getsystem Meterpreter/Cobalt Strike command by detecting a specific service starting
- category: data/rules/windows/process_creation
- level: high
- id: 15619216-e993-4721-b590-4c520615a67d

Title: Process Dump via Comsvcs DLL
- description: Detects process memory dump via comsvcs.dll and rundll32
- category: data/rules/windows/process_creation
- level: high
- id: 09e6d5c0-05b8-4ff8-9eeb-043046ec774c

Title: Emotet Process Creation
- description: Detects all Emotet like process executions that are not covered by the more generic rules
- category: data/rules/windows/process_creation
- level: critical
- id: d02e8cf5-6099-48cf-9bfc-1eec2d0c7b18

Title: IIS Native-Code Module Command Line Installation
- description: Detects suspicious IIS native-code module installations via command line
- category: data/rules/windows/process_creation
- level: medium
- id: 9465ddf4-f9e4-4ebd-8d98-702df3a93239

Title: Proxy Execution Via Explorer.exe
- description: Attackers can use explorer.exe for evading defense mechanisms
- category: data/rules/windows/process_creation
- level: low
- id: 9eb271b9-24ae-4cd4-9465-19cfc1047f3e

Title: Suspicious Execution of Shutdown

- description: Use of the commandline to shutdown or reboot windows
- category: data/rules/windows/process_creation
- level: medium
- id: 34ebb878-1b15-4895-b352-ca2eeb99b274

Title: Renamed PsExec
- description: Detects the execution of a renamed PsExec often used by attackers or malware
- category: data/rules/windows/process_creation
- level: high
- id: a7a7e0e5-1d57-49df-9c58-9fe5bc0346a2

Title: Cmdkey Cached Credentials Recon
- description: Detects usage of cmdkey to look for cached credentials
- category: data/rules/windows/process_creation
- level: high
- id: 07f8bdc2-c9b3-472a-9817-5a670b872f53

Title: Pingback Backdoor
- description: Detects the use of Pingback backdoor that creates ICMP tunnel for C2 as described in the trustwave report
- category: data/rules/windows/process_creation
- level: high
- id: b2400ffb-7680-47c0-b08a-098a7de7e7a9

Title: UAC Bypass WSReset
- description: Detects the pattern of UAC Bypass via WSReset usable by default sysmon-config
- category: data/rules/windows/process_creation
- level: high
- id: 89a9a0e0-f61a-42e5-8957-b1479565a658

Title: Audio Capture via SoundRecorder
- description: Detect attacker collecting audio via SoundRecorder application.
- category: data/rules/windows/process_creation
- level: medium
- id: 83865853-59aa-449e-9600-74b9d89a6d6e

Title: Excel Proxy Executing Regsvr32 With Payload
- description: Excel called wmic to finally proxy execute regsvr32 with the payload. An attacker wanted to break suspicious pa
- category: data/rules/windows/process_creation
- level: high
- id: 9d1c72f5-43f0-4da5-9320-648cf2099dd0

Title: UAC Bypass Tool UACMe
- description: Detects execution of UACMe (a tool used for UAC bypass) via default PE metadata
- category: data/rules/windows/process_creation
- level: high
- id: d38d2fa4-98e6-4a24-aff1-410b0c9ad177

Title: VeeamBackup Database Credentials Dump
- description: Detects dump of credentials in VeeamBackup dbo
- category: data/rules/windows/process_creation
- level: high
- id: b57ba453-b384-4ab9-9f40-1038086b4e53

Title: DarkSide Ransomware Pattern
- description: Detects DarkSide Ransomware and helpers
- category: data/rules/windows/process_creation
- level: critical
- id: 965fff6c-1d7e-4e25-91fd-cdccd75f7d2c

Title: Gpresult Display Group Policy Information
- description: Detects cases in which a user uses the built-in Windows utility gpresult to display the Resultant Set of Policy
- category: data/rules/windows/process_creation
- level: medium
- id: e56d3073-83ff-4021-90fe-c658e0709e72

Title: Tor Client or Tor Browser Use
- description: Detects the use of Tor or Tor-Browser to connect to onion routing networks
- category: data/rules/windows/process_creation
- level: high

- id: 62f7c9bf-9135-49b2-8aeb-1e54a6ecc13c

Title: Suspicious GUP Usage
- description: Detects execution of the Notepad++ updater in a suspicious directory, which is often used in DLL side-loading a
- category: data/rules/windows/process_creation
- level: high
- id: 0a4f6091-223b-41f6-8743-f322ec84930b

Title: Terminal Service Process Spawn
- description: Detects a process spawned by the terminal service server process (this could be an indicator for an exploitatio
- category: data/rules/windows/process_creation
- level: high
- id: 1012f107-b8f1-4271-af30-5aed2de89b39

Title: WMI Uninstall An Application
- description: Uninstall an application with wmic
- category: data/rules/windows/process_creation
- level: medium
- id: b53317a0-8acf-4fd1-8de8-a5401e776b96

Title: PowerShell Web Download and Execution
- description: Detects suspicious ways to download files or content using PowerShell
- category: data/rules/windows/process_creation
- level: high
- id: 85b0b087-eddf-4a2b-b033-d771fa2b9775

Title: Application Whitelisting Bypass via DLL Loaded by odbcconf.exe
- description: Detects defence evasion attempt via odbcconf.exe execution to load DLL
- category: data/rules/windows/process_creation
- level: medium
- id: 65d2be45-8600-4042-b4c0-577a1ff8a60e

Title: Suspicious File Download via CertOC.exe
- description: Detects when a user downloads file by using CertOC.exe
- category: data/rules/windows/process_creation
- level: high
- id: 70ad0861-d1fe-491c-a45f-fa48148a300d

Title: Windows Network Enumeration
- description: Identifies attempts to enumerate hosts in a network using the built-in Windows net.exe tool.
- category: data/rules/windows/process_creation
- level: low
- id: 62510e69-616b-4078-b371-847da438cc03

Title: CrackMapExec Process Patterns
- description: Detects suspicious process patterns found in logs when CrackMapExec is used
- category: data/rules/windows/process_creation
- level: high
- id: f26307d8-14cd-47e3-a26b-4b4769f24af6

Title: Detection of PowerShell Execution via Sqlps.exe
- description: This rule detects execution of a PowerShell code through the sqlps.exe utility, which is included in the standa
- category: data/rules/windows/process_creation
- level: medium
- id: 0152550d-3a26-4efd-9f0e-54a0b28ae2f3

Title: Change PowerShell Policies to an Unsecure Level
- description: Detects use of executionpolicy option to set a unsecure policies
- category: data/rules/windows/process_creation
- level: medium
- id: 87e3c4e8-a6a8-4ad9-bb4f-46e7ff99a180

Title: Audio Capture via PowerShell
- description: Detects audio capture via PowerShell Cmdlet.
- category: data/rules/windows/process_creation
- level: medium
- id: 932fb0d8-692b-4b0f-a26e-5643a50fe7d6

Title: Empire PowerShell Launch Parameters

- description: Detects suspicious powershell command line parameters used in Empire
- category: data/rules/windows/process_creation
- level: critical
- id: 79f4ede3-402e-41c8-bc3e-ebbf5f162581

Title: Compress Data and Lock With Password for Exfiltration With 7-ZIP
- description: An adversary may compress or encrypt data that is collected prior to exfiltration using 3rd party utilities
- category: data/rules/windows/process_creation
- level: medium
- id: 9fbf5927-5261-4284-a71d-f681029ea574

Title: Defrag Deactivation
- description: Detects the deactivation and disabling of the Scheduled defragmentation task as seen by Slingshot APT group
- category: data/rules/windows/process_creation
- level: medium
- id: 958d81aa-8566-4cea-a565-59ccd4df27b0

Title: Network Reconnaissance Activity
- description: Detects a set of suspicious network related commands often used in recon stages
- category: data/rules/windows/process_creation
- level: high
- id: e6313acd-208c-44fc-a0ff-db85d572e90e

Title: Suspicious Rundll32 Activity Invoking Sys File
- description: Detects suspicious process related to rundll32 based on command line that includes a *.sys file as seen being u
- category: data/rules/windows/process_creation
- level: high
- id: 731231b9-0b5d-4219-94dd-abb6959aa7ea

Title: Registry Defender Tampering
- description: Detects reg command lines that disable certain important features of Microsoft Defender
- category: data/rules/windows/process_creation
- level: high
- id: 452bce90-6fb0-43cc-97a5-affc283139b3

Title: Stop Or Remove Antivirus Service
- description: Adversaries may disable security tools to avoid possible detection of their tools and activities by stopping te
- category: data/rules/windows/process_creation
- level: medium
- id: 6783aa9e-0dc3-49d4-a94a-8b39c5fd700b

Title: Disable of ETW Trace
- description: Detects a command that clears or disables any ETW trace log which could indicate a logging evasion.
- category: data/rules/windows/process_creation
- level: high
- id: a238b5d0-ce2d-4414-a676-7a531b3d13d6

Title: Exports Registry Key To a File
- description: Detects the export of the target Registry key to a file.
- category: data/rules/windows/process_creation
- level: low
- id: f0e53e89-8d22-46ea-9db5-9d4796ee2f8a

Title: Cmd Stream Redirection
- description: Detects the redirection of an output stream of / within a Windows command line session
- category: data/rules/windows/process_creation
- level: low
- id: 70e68156-6571-427b-a6e9-4476a173a9b6

Title: QBot Process Creation
- description: Detects QBot like process executions
- category: data/rules/windows/process_creation
- level: critical
- id: 4fcac6eb-0287-4090-8eea-2602e4c20040

Title: WScript or CScript Dropper
- description: Detects wscript/cscript executions of scripts located in user directories
- category: data/rules/windows/process_creation
- level: high

- id: cea72823-df4d-4567-950c-0b579eaf0846

Title: Remove Windows Defender Definition Files
- description: Adversaries may disable security tools to avoid possible detection of their tools and activities by removing Wi
- category: data/rules/windows/process_creation
- level: medium
- id: 9719a8aa-401c-41af-8108-ced7ec9cd75c

Title: Suspicious ftp.exe
- description: Detects renamed ftp.exe, ftp.exe script execution and child processes ran by ftp.exe
- category: data/rules/windows/process_creation
- level: medium
- id: 06b401f4-107c-4ff9-947f-9ec1e7649f1e

Title: Logon Scripts (UserInitMprLogonScript)
- description: Detects creation or execution of UserInitMprLogonScript persistence method
- category: data/rules/windows/process_creation
- level: high
- id: 0a98a10c-685d-4ab0-bddc-b6bdd1d48458

Title: F-Secure C3 Load by Rundll32
- description: F-Secure C3 produces DLLs with a default exported StartNodeRelay function.
- category: data/rules/windows/process_creation
- level: critical
- id: b18c9d4c-fac9-4708-bd06-dd5bfacf200f

Title: Suspicious PowerShell Parameter Substring
- description: Detects suspicious PowerShell invocation with a parameter substring
- category: data/rules/windows/process_creation
- level: high
- id: 36210e0d-5b19-485d-a087-c096088885f0

Title: Invoke-Obfuscation COMPRESS OBFUSCATION
- description: Detects Obfuscated Powershell via COMPRESS OBFUSCATION
- category: data/rules/windows/process_creation
- level: medium
- id: 7eedcc9d-9fdb-4d94-9c54-474e8affc0c7

Title: Winword.exe Loads Suspicious DLL
- description: Detects Winword.exe loading of custmom dll via /l cmd switch
- category: data/rules/windows/process_creation
- level: medium
- id: 2621b3a6-3840-4810-ac14-a02426086171

Title: ShimCache Flush
- description: Detects actions that clear the local ShimCache and remove forensic evidence
- category: data/rules/windows/process_creation
- level: critical
- id: b0524451-19af-4efa-a46f-562a977f792e

Title: APT29
- description: This method detects a suspicious PowerShell command line combination as used by APT29 in a campaign against U.S
- category: data/rules/windows/process_creation
- level: critical
- id: 033fe7d6-66d1-4240-ac6b-28908009c71f

Title: Wbadmin Delete Systemstatebackup
- description: Deletes the Windows systemstatebackup using wbadmin.exe.

This technique is used by numerous ransomware families. This may only be successful on server platforms that have Windows Backup enabled.

- category: data/rules/windows/process_creation
- level: high
- id: 89f75308-5b1b-4390-b2d8-d6b2340efaf8

Title: Suspicious Add Scheduled Task From User AppData Temp
- description: schtasks.exe create task from user AppData\Local\Temp
- category: data/rules/windows/process_creation
- level: high

- id: 43f487f0-755f-4c2a-bce7-d6d2eec2fcf8

Title: PsExec/PAExec Escalation to LOCAL SYSTEM
- description: Detects suspicious flags used by PsExec and PAExec to escalate a command line to LOCAL_SYSTEM rights
- category: data/rules/windows/process_creation
- level: high
- id: 8834e2f7-6b4b-4f09-8906-d2276470ee23

Title: Renamed PAExec
- description: Detects suspicious renamed PAExec execution as often used by attackers
- category: data/rules/windows/process_creation
- level: high
- id: c4e49831-1496-40cf-8ce1-b53f942b02f9

Title: Encoded PowerShell Command Line
- description: Detects specific combinations of encoding methods in the PowerShell command lines
- category: data/rules/windows/process_creation
- level: medium
- id: cdf05894-89e7-4ead-b2b0-0a5f97a90f2f

Title: UAC Bypass Using ChangePK and SLUI
- description: Detects an UAC bypass that uses changepk.exe and slui.exe (UACMe 61)
- category: data/rules/windows/process_creation
- level: high
- id: 503d581c-7df0-4bbe-b9be-5840c0ecc1fc

Title: Format.com FileSystem LOLBIN
- description: Detects the execution of format.com with a suspicious filesystem selection that could indicate a defense evasio
- category: data/rules/windows/process_creation
- level: high
- id: 9fb6b26e-7f9e-4517-a48b-8cac4a1b6c60

Title: Netsh RDP Port Forwarding
- description: Detects netsh commands that configure a port forwarding of port 3389 used for RDP
- category: data/rules/windows/process_creation
- level: high
- id: 782d6f3e-4c5d-4b8c-92a3-1d05fed72e63

Title: Wlrmdr Lolbin Use as Laucher
- description: Detects use of Wlrmdr.exe in which the -u parameter is passed to ShellExecute
- category: data/rules/windows/process_creation
- level: medium
- id: 9cfc00b6-bfb7-49ce-9781-ef78503154bb

Title: Suspicious Listing of Network Connections
- description: Adversaries may attempt to get a listing of network connections to or from the compromised system they are curr
- category: data/rules/windows/process_creation
- level: low
- id: 1c67a717-32ba-409b-a45d-0fb704a73a81

Title: Non-privileged Usage of Reg or Powershell
- description: Search for usage of reg or Powershell by non-priveleged users to modify service configuration in registry
- category: data/rules/windows/process_creation
- level: high
- id: 8f02c935-effe-45b3-8fc9-ef8696a9e41d

Title: Renamed Whoami Execution
- description: Detects the execution of whoami that has been renamed to a different name to avoid detection
- category: data/rules/windows/process_creation
- level: critical
- id: f1086bf7-a0c4-4a37-9102-01e573caf4a0

Title: Suspicious Spool Service Child Process
- description: Detects suspicious print spool service (spoolsv.exe) child processes.
- category: data/rules/windows/process_creation
- level: high
- id: dcdbc940-0bff-46b2-95f3-2d73f848e33b

Title: Abusing Findstr for Defense Evasion

- description: Attackers can use findstr to hide their artifacts or search specific strings and evade defense mechanism
- category: data/rules/windows/process_creation
- level: medium
- id: bf6c39fc-e203-45b9-9538-05397c1b4f3f

Title: Suspicious Rundll32 Without Any CommandLine Params
- description: Detects suspicious start of rundll32.exe without any parameters as found in CobaltStrike beacon activity
- category: data/rules/windows/process_creation
- level: high
- id: 1775e15e-b61b-4d14-a1a3-80981298085a

Title: Detection of PowerShell Execution via DLL
- description: Detects PowerShell Strings applied to rundll as seen in PowerShdll.dll
- category: data/rules/windows/process_creation
- level: high
- id: 6812a10b-60ea-420c-832f-dfcc33b646ba

Title: MMC Spawning Windows Shell
- description: Detects a Windows command line executable started from MMC
- category: data/rules/windows/process_creation
- level: high
- id: 05a2ab7e-ce11-4b63-86db-ab32e763e11d

Title: Possible App Whitelisting Bypass via WinDbg/CDB as a Shellcode Runner
- description: Launch 64-bit shellcode from a debugger script file using cdb.exe.
- category: data/rules/windows/process_creation
- level: medium
- id: b5c7395f-e501-4a08-94d4-57fe7a9da9d2

Title: Application Whitelisting Bypass via Bginfo
- description: Execute VBscript code that is referenced within the *.bgi file.
- category: data/rules/windows/process_creation
- level: medium
- id: aaf46cdc-934e-4284-b329-34aa701e3771

Title: Suspicious Use of Procdump on LSASS
- description: Detects suspicious uses of the SysInternals Procdump utility by using a special command line parameter in combi
- category: data/rules/windows/process_creation
- level: critical
- id: 5afee48e-67dd-4e03-a783-f74259dcf998

Title: Suspicious Process Start Locations
- description: Detects suspicious process run from unusual locations
- category: data/rules/windows/process_creation
- level: medium
- id: 15b75071-74cc-47e0-b4c6-b43744a62a2b

Title: Change Default File Association
- description: When a file is opened, the default program used to open the file (also called the file association or handler)
- category: data/rules/windows/process_creation
- level: low
- id: 3d3aa6cd-6272-44d6-8afc-7e88dfef7061

Title: Using AppVLP To Circumvent ASR File Path Rule
- description: Application Virtualization Utility is included with Microsoft Office. We are able to abuse "AppVLP" to execute

Normally, this binary is used for Application Virtualization, but we can use it as an abuse binary to circumvent the ASR file path rule folder or to mark a file as a system file.

- category: data/rules/windows/process_creation
- level: medium
- id: 9c7e131a-0f2c-4ae0-9d43-b04f4e266d43

Title: DumpStack.log Defender Evasion
- description: Detects the use of the filename DumpStack.log to evade Microsoft Defender
- category: data/rules/windows/process_creation
- level: critical
- id: 4f647cfa-b598-4e12-ad69-c68dd16caef8

Title: Indirect Command Execution By Program Compatibility Wizard
- description: Detect indirect command execution via Program Compatibility Assistant pcwrun.exe
- category: data/rules/windows/process_creation
- level: low
- id: b97cd4b1-30b8-4a9d-bd72-6293928d52bc

Title: GatherNetworkInfo.vbs Script Usage
- description: Adversaries can abuse of C:\Windows\System32\gatherNetworkInfo.vbs script along with cscript.exe to gather info
- category: data/rules/windows/process_creation
- level: medium
- id: 575dce0c-8139-4e30-9295-1ee75969f7fe

Title: Suspicious LSASS Process Clone
- description: Detects a suspicious LSASS process process clone that could be a sign of process dumping activity
- category: data/rules/windows/process_creation
- level: critical
- id: c8da0dfd-4ed0-4b68-962d-13c9c884384e

Title: Disable Windows IIS HTTP Logging
- description: Disables HTTP logging on a Windows IIS web server as seen by Threat Group 3390 (Bronze Union)
- category: data/rules/windows/process_creation
- level: high
- id: e4ed6030-ffe5-4e6a-8a8a-ab3c1ab9d94e

Title: Net.exe User Account Creation
- description: Identifies creation of local users via the net.exe command.
- category: data/rules/windows/process_creation
- level: medium
- id: cd219ff3-fa99-45d4-8380-a7d15116c6dc

Title: Recon Information for Export with Command Prompt
- description: Once established within a system or network, an adversary may use automated techniques for collecting internal
- category: data/rules/windows/process_creation
- level: medium
- id: aa2efee7-34dd-446e-8a37-40790a66efd7

Title: Imports Registry Key From a File
- description: Detects the import of the specified file to the registry with regedit.exe.
- category: data/rules/windows/process_creation
- level: medium
- id: 73bba97f-a82d-42ce-b315-9182e76c57b1

Title: Mounted Windows Admin Shares with net.exe
- description: Detects when an admin share is mounted using net.exe
- category: data/rules/windows/process_creation
- level: medium
- id: 3abd6094-7027-475f-9630-8ab9be7b9725

Title: Renamed ProcDump
- description: Detects the execution of a renamed ProcDump executable often used by attackers or malware
- category: data/rules/windows/process_creation
- level: critical
- id: 4a0b2c7e-7cb2-495d-8b63-5f268e7bfd67

Title: Suspect Svchost Activity
- description: It is extremely abnormal for svchost.exe to spawn without any CLI arguments and is normally observed when a mal
- category: data/rules/windows/process_creation
- level: critical
- id: 16c37b52-b141-42a5-a3ea-bbe098444397

Title: Mimikatz Command Line
- description: Detection well-known mimikatz command line arguments
- category: data/rules/windows/process_creation
- level: medium
- id: a642964e-bead-4bed-8910-1bb4d63e3b4d

Title: Winnti Pipemon Characteristics
- description: Detects specific process characteristics of Winnti Pipemon malware reported by ESET
- category: data/rules/windows/process_creation

- level: critical
- id: 73d70463-75c9-4258-92c6-17500fe972f2

Title: Fsutil Drive Enumeration
- description: Attackers may leverage fsutil to enumerated connected drives.
- category: data/rules/windows/process_creation
- level: low
- id: 63de06b9-a385-40b5-8b32-73f2b9ef84b6

Title: CrackMapExec PowerShell Obfuscation
- description: The CrachMapExec pentesting framework implements a PowerShell obfuscation with some static strings detected by
- category: data/rules/windows/process_creation
- level: high
- id: 6f8b3439-a203-45dc-a88b-abf57ea15ccf

Title: WMIExec VBS Script
- description: Detects suspicious file execution by wscript and cscript
- category: data/rules/windows/process_creation
- level: critical
- id: 966e4016-627f-44f7-8341-f394905c361f

Title: Suspicious Nmap Execution
- description: Adversaries may attempt to get a listing of services running on remote hosts, including those that may be vulne
- category: data/rules/windows/process_creation
- level: high
- id: f6ecd1cf-19b8-4488-97f6-00f0924991a3

Title: Blue Mockingbird
- description: Attempts to detect system changes made by Blue Mockingbird
- category: data/rules/windows/process_creation
- level: high
- id: c3198a27-23a0-4c2c-af19-e5328d49680e

Title: Suspicious Usage of the Manage-bde.wsf Script
- description: Detects a usage of the manage-bde.wsf script that may indicate an attempt of proxy execution from script
- category: data/rules/windows/process_creation
- level: medium
- id: c363385c-f75d-4753-a108-c1a8e28bdbda

Title: CreateMiniDump Hacktool
- description: Detects the use of CreateMiniDump hack tool used to dump the LSASS process memory for credential extraction on
- category: data/rules/windows/process_creation
- level: high
- id: 36d88494-1d43-4dc0-b3fa-35c8fea0ca9d

Title: CobaltStrike Process Patterns
- description: Detects process patterns found in Cobalt Strike beacon activity (see reference for more details) and also cases
- category: data/rules/windows/process_creation
- level: high
- id: f35c5d71-b489-4e22-a115-f003df287317

Title: Schtasks From Suspicious Folders
- description: Detects scheduled task creations that have suspicious action command and folder combinations
- category: data/rules/windows/process_creation
- level: high
- id: 8a8379b8-780b-4dbf-b1e9-31c8d112fefb

Title: Suspicious Rundll32 Setupapi.dll Activity
- description: setupapi.dll library provide InstallHinfSection function for processing INF files. INF file may contain instruc
- category: data/rules/windows/process_creation
- level: medium
- id: 285b85b1-a555-4095-8652-a8a4106af63f

Title: Invoke-Obfuscation STDIN+ Launcher
- description: Detects Obfuscated use of stdin to execute PowerShell
- category: data/rules/windows/process_creation
- level: high
- id: 6c96fc76-0eb1-11eb-adc1-0242ac120002

Title: Suspicious ScreenSave Change by Reg.exe
- description: Adversaries may establish persistence by executing malicious content triggered by user inactivity.

Screensavers are programs that execute after a configurable time of user inactivity and consist of Portable Executable (PE) files with a .scr file extension

- category: data/rules/windows/process_creation
- level: medium
- id: 0fc35fc3-efe6-4898-8a37-0b233339524f

Title: SyncAppvPublishingServer VBS Execute Arbitrary PowerShell Code
- description: Executes arbitrary PowerShell code using SyncAppvPublishingServer.vbs
- category: data/rules/windows/process_creation
- level: medium
- id: 36475a7d-0f6d-4dce-9b01-6aeb473bbaf1

Title: Regsvr32 Anomaly
- description: Detects various anomalies in relation to regsvr32.exe
- category: data/rules/windows/process_creation
- level: high
- id: 8e2b24c9-4add-46a0-b4bb-0057b4e6187d

Title: Conti Ransomware Execution
- description: Conti ransomware command line ioc
- category: data/rules/windows/process_creation
- level: critical
- id: 689308fc-cfba-4f72-9897-796c1dc61487

Title: Verclsid.exe Runs COM Object
- description: Detects when verclsid.exe is used to run COM object via GUID
- category: data/rules/windows/process_creation
- level: medium
- id: d06be4b9-8045-428b-a567-740a26d9db25

Title: Enumeration for Credentials in Registry
- description: Adversaries may search the Registry on compromised systems for insecurely stored credentials.

The Windows Registry stores configuration information that can be used by the system or other programs. Adversaries may query the Registry looking for credentials and passwords that have been stored for use by other programs or services

- category: data/rules/windows/process_creation
- level: medium
- id: e0b0c2ab-3d52-46d9-8cb7-049dc775fbd1

Title: Microsoft Workflow Compiler
- description: Detects invocation of Microsoft Workflow Compiler, which may permit the execution of arbitrary unsigned code.
- category: data/rules/windows/process_creation
- level: high
- id: 419dbf2b-8a9b-4bea-bf99-7544b050ec8d

Title: Remote Procedure Call Service Anomaly
- description: Detects suspicious remote procedure call (RPC) service anomalies based on the spawned sub processes (long shot
- category: data/rules/windows/process_creation
- level: high
- id: a7cd7306-df8b-4398-b711-6f3e4935cf16

Title: Winrar Execution in Non-Standard Folder
- description: Detects a suspicious winrar execution in a folder which is not the default installation folder
- category: data/rules/windows/process_creation
- level: high
- id: 4ede543c-e098-43d9-a28f-dd784a13132f

Title: Base64 Encoded Reflective Assembly Load
- description: Detects base64 encoded .NET reflective loading of Assembly
- category: data/rules/windows/process_creation
- level: high
- id: 62b7ccc9-23b4-471e-aa15-6da3663c4d59

Title: Suspicious Findstr 385201 Execution
- description: Discovery of an installed Sysinternals Sysmon service using driver altitude (even if the name is changed).
- category: data/rules/windows/process_creation

- level: high
- id: 37db85d1-b089-490a-a59a-c7b6f984f480

Title: Winnti Malware HK University Campaign
- description: Detects specific process characteristics of Winnti malware noticed in Dec/Jan 2020 in a campaign against Honk K
- category: data/rules/windows/process_creation
- level: critical
- id: 3121461b-5aa0-4a41-b910-66d25524edbb

Title: Bad Opsec Defaults Sacrificial Processes With Improper Arguments
- description: Detects attackers using tooling with bad opsec defaults e.g. spawning a sacrificial process to inject a capabil
- category: data/rules/windows/process_creation
- level: high
- id: a7c3d773-caef-227e-a7e7-c2f13c622329

Title: HH.exe Execution
- description: Identifies usage of hh.exe executing recently modified .chm files.
- category: data/rules/windows/process_creation
- level: high
- id: 68c8acb4-1b60-4890-8e82-3ddf7a6dba84

Title: Suspicious Scheduled Task Creation Involving Temp Folder
- description: Detects the creation of scheduled tasks that involves a temporary folder and runs only once
- category: data/rules/windows/process_creation
- level: high
- id: 39019a4e-317f-4ce3-ae63-309a8c6b53c5

Title: Suspicious Curl File Upload
- description: Detects a suspicious curl process start the adds a file to a web request
- category: data/rules/windows/process_creation
- level: medium
- id: 00bca14a-df4e-4649-9054-3f2aa676bc04

Title: Office Applications Spawning Wmi Cli
- description: Initial execution of malicious document calls wmic to execute the file with regsvr32
- category: data/rules/windows/process_creation
- level: high
- id: 518643ba-7d9c-4fa5-9f37-baed36059f6a

Title: Windows 10 Scheduled Task SandboxEscaper 0-day
- description: Detects Task Scheduler .job import arbitrary DACL write\par
- category: data/rules/windows/process_creation
- level: high
- id: 931b6802-d6a6-4267-9ffa-526f57f22aaf

Title: Suspicious Kernel Dump Using Dtrace
- description: Detects suspicious way to dump the kernel on Windows systems using dtrace.exe, which is available on Windows sy
- category: data/rules/windows/process_creation
- level: high
- id: 7124aebe-4cd7-4ccb-8df0-6d6b93c96795

Title: Copy from Volume Shadow Copy
- description: Detects a copy execution that targets a shadow copy (sometimes used to copy registry hives that are in use)
- category: data/rules/windows/process_creation
- level: medium
- id: c73124a7-3e89-44a3-bdc1-25fe4df754b1

Title: Shadow Copies Access via Symlink
- description: Shadow Copies storage symbolic link creation using operating systems utilities
- category: data/rules/windows/process_creation
- level: medium
- id: 40b19fa6-d835-400c-b301-41f3a2baacaf

Title: UNC2452 Process Creation Patterns
- description: Detects a specific process creation patterns as seen used by UNC2452 and provided by Microsoft as Microsoft Def
- category: data/rules/windows/process_creation
- level: critical
- id: 9be34ad0-b6a7-4fbd-91cf-fc7ec1047f5f

Title: Suspicious Csi.exe Usage
- description: Csi.exe is a signed binary from Microsoft that comes with Visual Studio and provides C# interactive capabilitie
- category: data/rules/windows/process_creation
- level: medium
- id: 40b95d31-1afc-469e-8d34-9a3a667d058e

Title: Suspicious VBoxDrvInst.exe Parameters
- description: Detect VBoxDrvInst.exe run with parameters allowing processing INF file. This allows to create values in the re
- category: data/rules/windows/process_creation
- level: medium
- id: b7b19cb6-9b32-4fc4-a108-73f19acfe262

Title: Suspicious WMI Reconnaissance
- description: An adversary might use WMI to list Processes running on the compromised host or list installed Software hotfix
- category: data/rules/windows/process_creation
- level: medium
- id: 221b251a-357a-49a9-920a-271802777cc0

Title: Suspicious Where Execution
- description: Adversaries may enumerate browser bookmarks to learn more about compromised hosts.

Browser bookmarks may reveal personal information about users (ex: banking sites, interests, social media, etc.) as well as details about internal network resources such as servers, tools/dashboards, or other related infrastructure.

- category: data/rules/windows/process_creation
- level: low
- id: 725a9768-0f5e-4cb3-aec2-bc5719c6831a

Title: Using SettingSyncHost.exe as LOLBin
- description: Detects using SettingSyncHost.exe to run hijacked binary
- category: data/rules/windows/process_creation
- level: high
- id: b2ddd389-f676-4ac4-845a-e00781a48e5f

Title: Bloodhound and Sharphound Hack Tool
- description: Detects command line parameters used by Bloodhound and Sharphound hack tools
- category: data/rules/windows/process_creation
- level: high
- id: f376c8a7-a2d0-4ddc-aa0c-16c17236d962

Title: Suspicious Key Manager Access
- description: Detects the invocation of the Stored User Names and Passwords dialogue (Key Manager)
- category: data/rules/windows/process_creation
- level: high
- id: a4694263-59a8-4608-a3a0-6f8d3a51664c

Title: Webshell Detection With Command Line Keywords
- description: Detects certain command line parameters often used during reconnaissance activity via web shells
- category: data/rules/windows/process_creation
- level: high
- id: bed2a484-9348-4143-8a8a-b801c979301c

Title: Tap Installer Execution
- description: Well-known TAP software installation. Possible preparation for data exfiltration using tunneling techniques
- category: data/rules/windows/process_creation
- level: medium
- id: 99793437-3e16-439b-be0f-078782cf953d

Title: Suspicious Rundll32 Activity
- description: Detects suspicious process related to rundll32 based on arguments
- category: data/rules/windows/process_creation
- level: medium
- id: e593cf51-88db-4ee1-b920-37e89012a3c9

Title: Suspicious Auditpol Usage
- description: Threat actors can use auditpol binary to change audit policy configuration to impair detection capability. This
- category: data/rules/windows/process_creation
- level: high
- id: 0a13e132-651d-11eb-ae93-0242ac130002

Title: Hydra Password Guessing Hack Tool
- description: Detects command line parameters used by Hydra password guessing hack tool
- category: data/rules/windows/process_creation
- level: high
- id: aaafa146-074c-11eb-adc1-0242ac120002

Title: Hermetic Wiper TG Process Patterns
- description: This rule detects process execution patterns found in intrusions related to the Hermetic Wiper malware attacks
- category: data/rules/windows/process_creation
- level: high
- id: 2f974656-6d83-4059-bbdf-68ac5403422f

Title: Process Dump via RdrLeakDiag.exe
- description: Detects a process memory dump performed by RdrLeakDiag.exe
- category: data/rules/windows/process_creation
- level: high
- id: edadb1e5-5919-4e4c-8462-a9e643b02c4b

Title: UAC Bypass Using Disk Cleanup
- description: Detects the pattern of UAC Bypass using scheduled tasks and variable expansion of cleanmgr.exe (UACMe 34)
- category: data/rules/windows/process_creation
- level: high
- id: b697e69c-746f-4a86-9f59-7bfff8eab881

Title: Turla Group Lateral Movement
- description: Detects automated lateral movement by Turla group
- category: data/rules/windows/process_creation
- level: critical
- id: c601f20d-570a-4cde-a7d6-e17f99cb8e7f

Title: Password Provided In Command Line Of Net.exe
- description: Detects a when net.exe is called with a password in the command line
- category: data/rules/windows/process_creation
- level: medium
- id: d4498716-1d52-438f-8084-4a603157d131

Title: Run Once Task Execution as Configured in Registry
- description: This rule detects the execution of Run Once task as configured in the registry
- category: data/rules/windows/process_creation
- level: low
- id: 198effb6-6c98-4d0c-9ea3-451fa143c45c

Title: Sysinternals SDelete Delete File
- description: Use of SDelete to erase a file not the free space
- category: data/rules/windows/process_creation
- level: medium
- id: a4824fca-976f-4964-b334-0621379e84c4

Title: Suspicious Commandline Escape
- description: Detects suspicious process that use escape characters
- category: data/rules/windows/process_creation
- level: low
- id: f0cdd048-82dc-4f7a-8a7a-b87a52b6d0fd

Title: Suspicious Conhost Legacy Option
- description: ForceV1 asks for information directly from the kernel space. Conhost connects to the console application
- category: data/rules/windows/process_creation
- level: informational
- id: 3037d961-21e9-4732-b27a-637bcc7bf539

Title: Exchange Exploitation Activity
- description: Detects activity observed by different researchers to be HAFNIUM group activity (or related) on Exchange server
- category: data/rules/windows/process_creation
- level: high
- id: bbb2dedd-a0e3-46ab-ba6c-6c82ae7a9aa7

Title: Suspicious WMI Execution Using Rundll32
- description: Detects WMI executing rundll32

- category: data/rules/windows/process_creation
- level: high
- id: 3c89a1e8-0fba-449e-8f1b-8409d6267ec8

Title: Bypass UAC via CMSTP
- description: Detect commandline usage of Microsoft Connection Manager Profile Installer (cmstp.exe) to install specially for
- category: data/rules/windows/process_creation
- level: high
- id: e66779cc-383e-4224-a3a4-267eeb585c40

Title: Suspicious Recursif Takeown
- description: Adversaries can interact with the DACLs using built-in Windows commands takeown which can grant adversaries hig
- category: data/rules/windows/process_creation
- level: medium
- id: 554601fb-9b71-4bcc-abf4-21a611be4fde

Title: Execution of Renamed PaExec
- description: Detects execution of renamed paexec via imphash and executable product string
- category: data/rules/windows/process_creation
- level: medium
- id: 7b0666ad-3e38-4e3d-9bab-78b06de85f7b

Title: Application Whitelisting Bypass via Dxcap.exe
- description: Detects execution of of Dxcap.exe
- category: data/rules/windows/process_creation
- level: medium
- id: 60f16a96-db70-42eb-8f76-16763e333590

Title: DTRACK Process Creation
- description: Detects specific process parameters as seen in DTRACK infections
- category: data/rules/windows/process_creation
- level: critical
- id: f1531fa4-5b84-4342-8f68-9cf3fdbd83d4

Title: DNS Exfiltration and Tunneling Tools Execution
- description: Well-known DNS Exfiltration tools execution
- category: data/rules/windows/process_creation
- level: high
- id: 98a96a5a-64a0-4c42-92c5-489da3866cb0

Title: Suspicious Rundll32 Invoking Inline VBScript
- description: Detects suspicious process related to rundll32 based on command line that invokes inline VBScript as seen being
- category: data/rules/windows/process_creation
- level: high
- id: 1cc50f3f-1fc8-4acf-b2e9-6f172e1fdebd

Title: Mouse Lock Credential Gathering
- description: In Kaspersky's 2020 Incident Response Analyst Report they listed legitimate tool "Mouse Lock" as being used for
- category: data/rules/windows/process_creation
- level: medium
- id: c9192ad9-75e5-43eb-8647-82a0a5b493e3

Title: Abused Debug Privilege by Arbitrary Parent Processes
- description: Detection of unusual child processes by different system processes
- category: data/rules/windows/process_creation
- level: high
- id: d522eca2-2973-4391-a3e0-ef0374321dae

Title: Suspicious Subsystem for Linux Bash Execution
- description: Performs execution of specified file, can be used as a defensive evasion.
- category: data/rules/windows/process_creation
- level: medium
- id: 5edc2273-c26f-406c-83f3-f4d948e740dd

Title: Suspicious aspnet_compiler.exe Execution
- description: Execute C# code with the Build Provider and proper folder structure in place.
- category: data/rules/windows/process_creation
- level: medium
- id: a01b8329-5953-4f73-ae2d-aa01e1f35f00

Title: Malicious Base64 Encoded PowerShell Keywords in Command Lines
- description: Detects base64 encoded strings used in hidden malicious PowerShell command lines
- category: data/rules/windows/process_creation
- level: high
- id: f26c6093-6f14-4b12-800f-0fcb46f5ffd0

Title: Sdclt Child Processes
- description: A General detection for sdclt spawning new processes. This could be an indicator of sdclt being used for bypass
- category: data/rules/windows/process_creation
- level: medium
- id: da2738f2-fadb-4394-afa7-0a0674885afa

Title: Suspicious SYSVOL Domain Group Policy Access
- description: Detects Access to Domain Group Policies stored in SYSVOL
- category: data/rules/windows/process_creation
- level: medium
- id: 05f3c945-dcc8-4393-9f3d-af65077a8f86

Title: Enabling RDP Service via Reg.exe
- description: Detects the execution of reg.exe and subsequent command line arguments for enabling RDP service on the host
- category: data/rules/windows/process_creation
- level: high
- id: 0d5675be-bc88-4172-86d3-1e96a4476536

Title: Elise Backdoor
- description: Detects Elise backdoor acitivty as used by APT32
- category: data/rules/windows/process_creation
- level: critical
- id: e507feb7-5f73-4ef6-a970-91bb6f6d744f

Title: UAC Bypass Using MSConfig Token Modification - Process
- description: Detects the pattern of UAC Bypass using a msconfig GUI hack (UACMe 55)
- category: data/rules/windows/process_creation
- level: high
- id: ad92e3f9-7eb6-460e-96b1-582b0ccbb980

Title: PsExec Service Start
- description: Detects a PsExec service start
- category: data/rules/windows/process_creation
- level: low
- id: 3ede524d-21cc-472d-a3ce-d21b568d8db7

Title: Regsvr32 Command Line Without DLL
- description: Detects a regsvr.exe execution that doesn't contain a DLL in the command line
- category: data/rules/windows/process_creation
- level: high
- id: 50919691-7302-437f-8e10-1fe088afa145

Title: Suspicious Atbroker Execution
- description: Atbroker executing non-deafualt Assistive Technology applications
- category: data/rules/windows/process_creation
- level: high
- id: f24bcaea-0cd1-11eb-adc1-0242ac120002

Title: Process Dump via Rundll32 and Comsvcs.dll
- description: Detects a process memory dump performed via ordinal function 24 in comsvcs.dll
- category: data/rules/windows/process_creation
- level: high
- id: 646ea171-dded-4578-8a4d-65e9822892e3

Title: DLL Execution Via Register-cimprovider.exe
- description: Detects using register-cimprovider.exe to execute arbitrary dll file.
- category: data/rules/windows/process_creation
- level: medium
- id: a2910908-e86f-4687-aeba-76a5f996e652

Title: Suspicious Execution of SharpView Aka PowerView
- description: Adversaries may look for details about the network configuration and settings of systems they access or through

- category: data/rules/windows/process_creation
- level: high
- id: b2317cfa-4a47-4ead-b3ff-297438c0bc2d

Title: Suspicious Serv-U Process Pattern
- description: Detects a suspicious process pattern which could be a sign of an exploited Serv-U service
- category: data/rules/windows/process_creation
- level: critical
- id: 58f4ea09-0fc2-4520-ba18-b85c540b0eaf

Title: Suspicious WebDav Client Execution
- description: Detects a privilege elevation attempt by coercing NTLM authentication on the Printer Spooler service
- category: data/rules/windows/process_creation
- level: high
- id: bb76d96b-821c-47cf-944b-7ce377864492

Title: Powershell Defender Base64 MpPreference
- description: Detects base64 encoded PowerShell code that modifies Windows Defender
- category: data/rules/windows/process_creation
- level: high
- id: c6fb44c6-71f5-49e6-9462-1425d328aee3

Title: Suspicious Execution of Powershell with Base64
- description: Commandline to lauch powershell with a base64 payload
- category: data/rules/windows/process_creation
- level: medium
- id: fb843269-508c-4b76-8b8d-88679db22ce7

Title: Equation Group DLL_U Load
- description: Detects a specific tool and export used by EquationGroup
- category: data/rules/windows/process_creation
- level: critical
- id: d465d1d8-27a2-4cca-9621-a800f37cf72e

Title: Non Interactive PowerShell
- description: Detects non-interactive PowerShell activity by looking at powershell.exe with not explorer.exe as a parent.
- category: data/rules/windows/process_creation
- level: low
- id: f4bbd493-b796-416e-bbf2-121235348529

Title: Pandemic Registry Key
- description: Detects Pandemic Windows Implant
- category: data/rules/windows/process_creation
- level: critical
- id: 9fefd33c-339d-4495-9cba-b96ca006f512

Title: Run Whoami as Privileged User
- description: Detects a whoami.exe executed by privileged accounts that are often misused by threat actors
- category: data/rules/windows/process_creation
- level: high
- id: 79ce34ca-af29-4d0e-b832-fc1b377020db

Title: Execution via stordiag.exe
- description: Detects the use of stordiag.exe to execute schtasks.exe systeminfo.exe and fltmc.exe
- category: data/rules/windows/process_creation
- level: high
- id: 961e0abb-1b1e-4c84-a453-aafe56ad0d34

Title: Use of LogMeIn Remote Access Software
- description: An adversary may use legitimate desktop support and remote access software, such as Team Viewer, Go2Assist, Log

These services are commonly used as legitimate technical support software, and may be allowed by application control within a target environment. Remote access tools like VNC, Ammyy, and Teamviewer are used frequently when compared with other legitimate software commonly used by adversaries. (Citation: Symantec Living off the Land)

- category: data/rules/windows/process_creation
- level: medium
- id: d85873ef-a0f8-4c48-a53a-6b621f11729d

Title: Droppers Exploiting CVE-2017-11882
- description: Detects exploits that use CVE-2017-11882 to start EQNEDT32.EXE and other sub processes like mshta.exe
- category: data/rules/windows/process_creation
- level: critical
- id: 678eb5f4-8597-4be6-8be7-905e4234b53a

Title: Taskmgr as LOCAL_SYSTEM
- description: Detects the creation of taskmgr.exe process in context of LOCAL_SYSTEM
- category: data/rules/windows/process_creation
- level: high
- id: 9fff585c-c33e-4a86-b3cd-39312079a65f

Title: Suspicious MSHTA Process Patterns
- description: Detects suspicious mshta process patterns
- category: data/rules/windows/process_creation
- level: high
- id: e32f92d1-523e-49c3-9374-bdb13b46a3ba

Title: Suspicious AdvancedRun Execution
- description: Detects the execution of AdvancedRun utitlity
- category: data/rules/windows/process_creation
- level: medium
- id: d2b749ee-4225-417e-b20e-a8d2193cbb84

Title: Excel Proxy Executing Regsvr32 With Payload
- description: Excel called wmic to finally proxy execute regsvr32 with the payload. An attacker wanted to break suspicious pa
- category: data/rules/windows/process_creation
- level: high
- id: c0e1c3d5-4381-4f18-8145-2583f06a1fe5

Title: Psr.exe Capture Screenshots
- description: The psr.exe captures desktop screenshots and saves them on the local machine
- category: data/rules/windows/process_creation
- level: medium
- id: 2158f96f-43c2-43cb-952a-ab4580f32382

Title: Modification of Boot Configuration
- description: Identifies use of the bcdedit command to delete boot configuration data. This tactic is sometimes used as by ma
- category: data/rules/windows/process_creation
- level: high
- id: 1444443e-6757-43e4-9ea4-c8fc705f79a2

Title: UNC2452 PowerShell Pattern
- description: Detects a specific PowerShell command line pattern used by the UNC2452 actors as mentioned in Microsoft and Sym
- category: data/rules/windows/process_creation
- level: critical
- id: b7155193-8a81-4d8f-805d-88de864ca50c

Title: Shell32 DLL Execution in Suspicious Directory
- description: Detects shell32.dll executing a DLL in a suspicious directory
- category: data/rules/windows/process_creation
- level: high
- id: 32b96012-7892-429e-b26c-ac2bf46066ff

Title: Remote PowerShell Session Host Process (WinRM)
- description: Detects remote PowerShell sections by monitoring for wsmprovhost (WinRM host process) as a parent or child proc
- category: data/rules/windows/process_creation
- level: medium
- id: 734f8d9b-42b8-41b2-bcf5-abaf49d5a3c8

Title: HTML Help Shell Spawn
- description: Detects a suspicious child process of a Microsoft HTML Help system when executing compiled HTML files (.chm)
- category: data/rules/windows/process_creation
- level: high
- id: 52cad028-0ff0-4854-8f67-d25dfcbc78b4

Title: Suspicious RASdial Activity
- description: Detects suspicious process related to rasdial.exe
- category: data/rules/windows/process_creation

- level: medium
- id: 6bba49bf-7f8c-47d6-a1bb-6b4dece4640e

Title: WMI Persistence - Script Event Consumer
- description: Detects WMI script event consumers
- category: data/rules/windows/process_creation
- level: high
- id: ec1d5e28-8f3b-4188-a6f8-6e8df81dc28e

Title: MMC20 Lateral Movement
- description: Detects MMC20.Application Lateral Movement; specifically looks for the spawning of the parent MMC.exe with a co
- category: data/rules/windows/process_creation
- level: high
- id: f1f3bf22-deb2-418d-8cce-e1a45e46a5bd

Title: Exfiltration and Tunneling Tools Execution
- description: Execution of well known tools for data exfiltration and tunneling
- category: data/rules/windows/process_creation
- level: medium
- id: c75309a3-59f8-4a8d-9c2c-4c927ad50555

Title: Suspicious Regsvr32 Execution With Image Extension
- description: utilizes REGSVR32.exe to execute this DLL masquerading as a Image file
- category: data/rules/windows/process_creation
- level: high
- id: 089fc3d2-71e8-4763-a8a5-c97fbb0a403e

Title: Sysmon Driver Unload
- description: Detect possible Sysmon driver unload
- category: data/rules/windows/process_creation
- level: high
- id: 4d7cda18-1b12-4e52-b45c-d28653210df8

Title: Atlassian Confluence CVE-2021-26084
- description: Detects spawning of suspicious child processes by Atlassian Confluence server which may indicate successful exp
- category: data/rules/windows/process_creation
- level: high
- id: 245f92e3-c4da-45f1-9070-bc552e06db11

Title: Suspicious Explorer Child Of Regsvr32
- description: Suspicious explorer.exe child of regsvr32.exe
- category: data/rules/windows/process_creation
- level: high
- id: 6f0947a4-1c5e-4e0d-8ac7-53159b8f23ca

Title: Wmiprvse Spawning Process
- description: Detects wmiprvse spawning processes
- category: data/rules/windows/process_creation
- level: high
- id: d21374ff-f574-44a7-9998-4a8c8bf33d7d

Title: NSudo Tool Execution As System
- description: Detects the use of NSudo tool for command execution
- category: data/rules/windows/process_creation
- level: high
- id: 771d1eb5-9587-4568-95fb-9ec44153a012

Title: DLL Injection with Tracker.exe
- description: This rule detects DLL injection and execution via LOLBAS - Tracker.exe
- category: data/rules/windows/process_creation
- level: medium
- id: 148431ce-4b70-403d-8525-fcc2993f29ea

Title: Ping Hex IP
- description: Detects a ping command that uses a hex encoded IP address
- category: data/rules/windows/process_creation
- level: high
- id: 1a0d4aba-7668-4365-9ce4-6d79ab088dfd

Title: NirCmd Tool Execution
- description: Detects the use of NirCmd tool for command execution, which could be the result of legitimate administrative ac
- category: data/rules/windows/process_creation
- level: medium
- id: 4e2ed651-1906-4a59-a78a-18220fca1b22

Title: Lazarus Session Highjacker
- description: Detects executables launched outside their default directories as used by Lazarus Group (Bluenoroff)
- category: data/rules/windows/process_creation
- level: high
- id: 3f7f5b0b-5b16-476c-a85f-ab477f6dd24b

Title: Dropping Of Password Filter DLL
- description: Detects dropping of dll files in system32 that may be used to retrieve user credentials from LSASS
- category: data/rules/windows/process_creation
- level: medium
- id: b7966f4a-b333-455b-8370-8ca53c229762

Title: SILENTTRINITY Stager Execution
- description: Detects SILENTTRINITY stager use
- category: data/rules/windows/process_creation
- level: high
- id: 03552375-cc2c-4883-bbe4-7958d5a980be

Title: Suspicious Load DLL via CertOC.exe
- description: Detects when a user installs certificates by using CertOC.exe to loads the target DLL file.
- category: data/rules/windows/process_creation
- level: medium
- id: 242301bc-f92f-4476-8718-78004a6efd9f

Title: Possible Privilege Escalation via Weak Service Permissions
- description: Detection of sc.exe utility spawning by user with Medium integrity level to change service ImagePath or Failure
- category: data/rules/windows/process_creation
- level: high
- id: d937b75f-a665-4480-88a5-2f20e9f9b22a

Title: MS Office Product Spawning Exe in User Dir
- description: Detects an executable in the users directory started from Microsoft Word, Excel, Powerpoint, Publisher or Visio
- category: data/rules/windows/process_creation
- level: high
- id: aa3a6f94-890e-4e22-b634-ffdfd54792cc

Title: Reg Disable Security Service
- description: Detects a suspicious reg.exe invocation that looks as if it would disable an important security service
- category: data/rules/windows/process_creation
- level: high
- id: 5e95028c-5229-4214-afae-d653d573d0ec

Title: UAC Bypass Using Consent and Comctl32 - Process
- description: Detects the pattern of UAC Bypass using consent.exe and comctl32.dll (UACMe 22)
- category: data/rules/windows/process_creation
- level: high
- id: 1ca6bd18-0ba0-44ca-851c-92ed89a61085

Title: WMI Spawning Windows PowerShell
- description: Detects WMI spawning PowerShell
- category: data/rules/windows/process_creation
- level: high
- id: 692f0bec-83ba-4d04-af7e-e884a96059b6

Title: Microsoft Office Product Spawning Windows Shell
- description: Detects a Windows command and scripting interpreter executable started from Microsoft Word, Excel, Powerpoint,
- category: data/rules/windows/process_creation
- level: high
- id: 438025f9-5856-4663-83f7-52f878a70a50

Title: Windows Update Client LOLBIN
- description: Detects code execution via the Windows Update client (wuauclt)
- category: data/rules/windows/process_creation

- level: high
- id: d7825193-b70a-48a4-b992-8b5b3015cc11

Title: SQLite Firefox Cookie DB Access
- description: Detect use of sqlite binary to query the Firefox cookies.sqlite database and steal the cookie data contained wi
- category: data/rules/windows/process_creation
- level: high
- id: 4833155a-4053-4c9c-a997-777fcea0baa7

Title: Suspicious Runscripthelper.exe
- description: Detects execution of powershell scripts via Runscripthelper.exe
- category: data/rules/windows/process_creation
- level: medium
- id: eca49c87-8a75-4f13-9c73-a5a29e845f03

Title: Empire Monkey
- description: Detects EmpireMonkey APT reported Activity
- category: data/rules/windows/process_creation
- level: critical
- id: 10152a7b-b566-438f-a33c-390b607d1c8d

Title: Whoami Execution Anomaly
- description: Detects the execution of whoami with suspicious parents or parameters
- category: data/rules/windows/process_creation
- level: high
- id: 8de1cbe8-d6f5-496d-8237-5f44a721c7a0

Title: UAC Bypass Using DismHost
- description: Detects the pattern of UAC Bypass using DismHost DLL hijacking (UACMe 63)
- category: data/rules/windows/process_creation
- level: high
- id: 853e74f9-9392-4935-ad3b-2e8c040dae86

Title: Set Windows System File with Attrib
- description: Marks a file as a system file using the attrib.exe utility
- category: data/rules/windows/process_creation
- level: low
- id: bb19e94c-59ae-4c15-8c12-c563d23fe52b

Title: Windows Credential Editor
- description: Detects the use of Windows Credential Editor (WCE)
- category: data/rules/windows/process_creation
- level: critical
- id: 7aa7009a-28b9-4344-8c1f-159489a390df

Title: Webshell Recon Detection Via CommandLine & Processes
- description: Looking for processes spawned by web server components that indicate reconnaissance by popular public domain we
- category: data/rules/windows/process_creation
- level: high
- id: f64e5c19-879c-4bae-b471-6d84c8339677

Title: DNSCat2 Powershell Implementation Detection Via Process Creation
- description: The PowerShell implementation of DNSCat2 calls nslookup to craft queries. Counting nslookup processes spawned b
- category: data/rules/windows/process_creation
- level: high
- id: b11d75d6-d7c1-11ea-87d0-0242ac130003

Title: Remote Code Execute via Winrm.vbs
- description: Detects an attempt to execute code or create service on remote host via winrm.vbs.
- category: data/rules/windows/process_creation
- level: medium
- id: 9df0dd3a-1a5c-47e3-a2bc-30ed177646a0

Title: Raccine Uninstall
- description: Detects commands that indicate a Raccine removal from an end system. Raccine is a free ransomware protection to
- category: data/rules/windows/process_creation
- level: high
- id: a31eeaed-3fd5-478e-a8ba-e62c6b3f9ecc

Title: Sticky Key Like Backdoor Usage
- description: Detects the usage and installation of a backdoor that uses an option to register a malicious debugger for built
- category: data/rules/windows/process_creation
- level: critical
- id: 2fdefcb3-dbda-401e-ae23-f0db027628bc

Title: Stop Windows Service
- description: Detects a windows service to be stopped
- category: data/rules/windows/process_creation
- level: low
- id: eb87818d-db5d-49cc-a987-d5da331fbd90

Title: DNS Tunnel Technique from MuddyWater
- description: Detecting DNS tunnel activity for Muddywater actor
- category: data/rules/windows/process_creation
- level: critical
- id: 36222790-0d43-4fe8-86e4-674b27809543

Title: Invoke-Obfuscation Via Use Clip
- description: Detects Obfuscated Powershell via use Clip.exe in Scripts
- category: data/rules/windows/process_creation
- level: high
- id: e1561947-b4e3-4a74-9bdd-83baed21bdb5

Title: Suspicious Cmdl32 Execution
- description: lolbas Cmdl32 is use to download a payload to evade test
- category: data/rules/windows/process_creation
- level: medium
- id: f37aba28-a9e6-4045-882c-d5004043b337

Title: SystemNightmare Exploitation Script Execution
- description: Detects the exploitation of PrinterNightmare to get a shell as LOCAL_SYSTEM
- category: data/rules/windows/process_creation
- level: critical
- id: c01f7bd6-0c1d-47aa-9c61-187b91273a16

Title: Gpscript Execution
- description: Detects the execution of the LOLBIN gpscript, which executes logon or startup scripts configured in Group Polic
- category: data/rules/windows/process_creation
- level: medium
- id: 1e59c230-6670-45bf-83b0-98903780607e

Title: Suspicious 7zip Subprocess
- description: 7-Zip through 21.07 on Windows allows privilege escalation (CVE-2022-29072) and command execution when a file w
- category: data/rules/windows/process_creation
- level: high
- id: 9a4ccd1a-3526-4d99-b980-9f9c5d3a6ee3

Title: WannaCry Ransomware
- description: Detects WannaCry ransomware activity
- category: data/rules/windows/process_creation
- level: critical
- id: 41d40bff-377a-43e2-8e1b-2e543069e079

Title: Invoke-Obfuscation VAR++ LAUNCHER OBFUSCATION
- description: Detects Obfuscated Powershell via VAR++ LAUNCHER
- category: data/rules/windows/process_creation
- level: high
- id: e9f55347-2928-4c06-88e5-1a7f8169942e

Title: Suspicious PowerShell Mailbox Export to Share
- description: Detects a PowerShell New-MailboxExportRequest that exports a mailbox to a local share, as used in ProxyShell ex
- category: data/rules/windows/process_creation
- level: critical
- id: 889719ef-dd62-43df-86c3-768fb08dc7c0

Title: Firewall Disabled via Netsh
- description: Detects netsh commands that turns off the Windows firewall
- category: data/rules/windows/process_creation

- level: medium
- id: 57c4bf16-227f-4394-8ec7-1b745ee061c3

Title: Suspicious Curl Usage on Windows
- description: Detects a suspicious curl process start on Windows and outputs the requested document to a local file
- category: data/rules/windows/process_creation
- level: medium
- id: e218595b-bbe7-4ee5-8a96-f32a24ad3468

Title: Windows Defender Download Activity
- description: Detect the use of Windows Defender to download payloads
- category: data/rules/windows/process_creation
- level: high
- id: 46123129-1024-423e-9fae-43af4a0fa9a5

Title: Suspicious Use of Procdump
- description: Detects suspicious uses of the SysInternals Procdump utility by using a special command line parameter ' -ma '
- category: data/rules/windows/process_creation
- level: high
- id: 03795938-1387-481b-9f4c-3f6241e604fe

Title: Disable Important Scheduled Task
- description: Adversaries may stop services or processes in order to conduct Data Destruction or Data Encrypted for Impact on
- category: data/rules/windows/process_creation
- level: high
- id: 9ac94dc8-9042-493c-ba45-3b5e7c86b980

Title: Interactive AT Job
- description: Detect an interactive AT job, which may be used as a form of privilege escalation.
- category: data/rules/windows/process_creation
- level: high
- id: 60fc936d-2eb0-4543-8a13-911c750a1dfc

Title: Suspicious Shells Spawn by SQL Server
- description: Detects suspicious shell spawn from MSSQL process, this might be sight of RCE or SQL Injection
- category: data/rules/windows/process_creation
- level: critical
- id: 869b9ca7-9ea2-4a5a-8325-e80e62f75445

Title: Suspicious Msiexec Load DLL
- description: Detects MsiExec loading a DLL and calling its DllUnregisterServer function
- category: data/rules/windows/process_creation
- level: medium
- id: 84f52741-8834-4a8c-a413-2eb2269aa6c8

Title: Empire PowerShell UAC Bypass
- description: Detects some Empire PowerShell UAC bypass methods
- category: data/rules/windows/process_creation
- level: critical
- id: 3268b746-88d8-4cd3-bffc-30077d02c787

Title: Rundll32 Registered COM Objects
- description: load malicious registered COM objects
- category: data/rules/windows/process_creation
- level: high
- id: f1edd233-30b5-4823-9e6a-c4171b24d316

Title: Devtoolslauncher.exe Executes Specified Binary
- description: The Devtoolslauncher.exe executes other binary
- category: data/rules/windows/process_creation
- level: critical
- id: cc268ac1-42d9-40fd-9ed3-8c4e1a5b87e6

Title: Advanced Port Scanner
- description: Detects the use of Advanced Port Scanner.
- category: data/rules/windows/process_creation
- level: medium
- id: 54773c5f-f1cc-4703-9126-2f797d96a69d

```
Title: Ps.exe Renamed SysInternals Tool
- description: Detects renamed SysInternals tool execution with a binary named ps.exe as used by Dragonfly APT group and docum
- category: data/rules/windows/process_creation
- level: high
- id: 18da1007-3f26-470f-875d-f77faf1cab31

Title: Fsutil Behavior Set SymlinkEvaluation
- description: A symbolic link is a type of file that contains a reference to another file.
```

This is probably done to make sure that the ransomware is able to follow shortcuts on the machine in order to find the original file to encrypt

```
- category: data/rules/windows/process_creation
- level: medium
- id: c0b2768a-dd06-4671-8339-b16ca8d1f27f

Title: LSASS Memory Dumping
- description: Detect creation of dump files containing the memory space of lsass.exe, which contains sensitive credentials. I
- category: data/rules/windows/process_creation
- level: high
- id: ffa6861c-4461-4f59-8a41-578c39f3f23e

Title: Suspicious Copy From or To System32
- description: Detects a suspicious copy command that copies a system program from System32 to another directory on disk - som
- category: data/rules/windows/process_creation
- level: medium
- id: fff9d2b7-e11c-4a69-93d3-40ef66189767

Title: Wsreset UAC Bypass
- description: Detects a method that uses Wsreset.exe tool that can be used to reset the Windows Store to bypass UAC
- category: data/rules/windows/process_creation
- level: high
- id: bdc8918e-a1d5-49d1-9db7-ea0fd91aa2ae

Title: Suspicious Rundll32 Script in CommandLine
- description: Detects suspicious process related to rundll32 based on arguments
- category: data/rules/windows/process_creation
- level: medium
- id: 73fcad2e-ff14-4c38-b11d-4172c8ac86c7

Title: Windows Hacktool Imphash
- description: Detects the use of Windows hacktools based on their import hash (imphash) even if the files have been renamed
- category: data/rules/windows/process_creation
- level: high
- id: 24e3e58a-646b-4b50-adef-02ef935b9fc8

Title: Fireball Archer Install
- description: Detects Archer malware invocation via rundll32
- category: data/rules/windows/process_creation
- level: high
- id: 3d4aebe0-6d29-45b2-a8a4-3dfde586a26d

Title: Execution via CL_Mutexverifiers.ps1
- description: Detects Execution via runAfterCancelProcess in CL_Mutexverifiers.ps1 module
- category: data/rules/windows/process_creation
- level: high
- id: 99465c8f-f102-4157-b11c-b0cddd53b79a

Title: SquiblyTwo
- description: Detects WMI SquiblyTwo Attack with possible renamed WMI by looking for imphash
- category: data/rules/windows/process_creation
- level: medium
- id: 8d63dadf-b91b-4187-87b6-34a1114577ea

Title: PowerShell Get-Process LSASS
- description: Detects a Get-Process command on lsass process, which is in almost all cases a sign of malicious activity
- category: data/rules/windows/process_creation
- level: high
- id: b2815d0d-7481-4bf0-9b6c-a4c48a94b349
```

Title: Windows Shell Spawning Suspicious Program
- description: Detects a suspicious child process of a Windows shell
- category: data/rules/windows/process_creation
- level: high
- id: 3a6586ad-127a-4d3b-a677-1e6eacdf8fde

Title: PowerShell Download from URL
- description: Detects a Powershell process that contains download commands in its command line string
- category: data/rules/windows/process_creation
- level: medium
- id: 3b6ab547-8ec2-4991-b9d2-2b06702a48d7

Title: Execution of Suspicious File Type Extension
- description: Checks whether the image specified in a process creation event doesn't refer to an .exe file (caused by process
- category: data/rules/windows/process_creation
- level: high
- id: c09dad97-1c78-4f71-b127-7edb2b8e491a

Title: Suspicious Service DACL Modification
- description: Detects suspicious DACL modifications that can be used to hide services or make them unstopable
- category: data/rules/windows/process_creation
- level: high
- id: 99cf1e02-00fb-4c0d-8375-563f978dfd37

Title: RedMimicry Winnti Playbook Execute
- description: Detects actions caused by the RedMimicry Winnti playbook
- category: data/rules/windows/process_creation
- level: high
- id: 95022b85-ff2a-49fa-939a-d7b8f56eeb9b

Title: CMSTP UAC Bypass via COM Object Access
- description: Detects UAC Bypass Attempt Using Microsoft Connection Manager Profile Installer Autoelevate-capable COM Objects
- category: data/rules/windows/process_creation
- level: high
- id: 4b60e6f2-bf39-47b4-b4ea-398e33cfe253

Title: Monitoring Wuauclt.exe For Lolbas Execution Of DLL
- description: Adversaries can abuse wuauclt.exe (Windows Update client) to run code execution by specifying an arbitrary DLL.
- category: data/rules/windows/process_creation
- level: medium
- id: ba1bb0cb-73da-42de-ad3a-de10c643a5d0

Title: Conti Volume Shadow Listing
- description: Detects a command used by conti to find volume shadow backups
- category: data/rules/windows/process_creation
- level: high
- id: 7b30e0a7-c675-4b24-8a46-82fa67e2433d

Title: UAC Bypass via Event Viewer
- description: Detects UAC bypass method using Windows event viewer
- category: data/rules/windows/process_creation
- level: critical
- id: be344333-921d-4c4d-8bb8-e584cf584780

Title: Winrar Compressing Dump Files
- description: Detects a suspicious winrar execution that involves a file with a .dmp extension, which could be a step in a pr
- category: data/rules/windows/process_creation
- level: high
- id: 1ac14d38-3dfc-4635-92c7-e3fd1c5f5bfc

Title: Application Whitelisting Bypass via Dnx.exe
- description: Execute C# code located in the consoleapp folder
- category: data/rules/windows/process_creation
- level: medium
- id: 81ebd28b-9607-4478-bf06-974ed9d53ed7

Title: Suspicious Execution of Adidnsdump
- description: This tool enables enumeration and exporting of all DNS records in the zone for recon purposes of internal netwo

Usee to Query/modify DNS records for Active Directory integrated DNS via LDAP

- category: data/rules/windows/process_creation
- level: low
- id: 26d3f0a2-f514-4a3f-a8a7-e7e48a8d9160

Title: PrintBrm ZIP Creation of Extraction
- description: Detects the execution of the LOLBIN PrintBrm.exe, which can be used to create or extract ZIP files. PrintBrm.ex
- category: data/rules/windows/process_creation
- level: high
- id: cafeeba3-01da-4ab4-b6c4-a31b1d9730c7

Title: Detected Windows Software Discovery
- description: Adversaries may attempt to enumerate software for a variety of reasons, such as figuring out what security meas
- category: data/rules/windows/process_creation
- level: medium
- id: e13f668e-7f95-443d-98d2-1816a7648a7b

Title: Judgement Panda Credential Access Activity
- description: Detects Russian group activity as described in Global Threat Report 2019 by Crowdstrike
- category: data/rules/windows/process_creation
- level: critical
- id: b83f5166-9237-4b5e-9cd4-7b5d52f4d8ee

Title: Suspicious Tasklist Discovery Command
- description: Adversaries may attempt to get information about running processes on a system. Information obtained could be u
- category: data/rules/windows/process_creation
- level: low
- id: 63332011-f057-496c-ad8d-d2b6afb27f96

Title: Adwind RAT / JRAT
- description: Detects javaw.exe in AppData folder as used by Adwind / JRAT
- category: data/rules/windows/process_creation
- level: high
- id: 1fac1481-2dbc-48b2-9096-753c49b4ec71

Title: Wmic Uninstall Security Product
- description: Detects deinstallation of security products using WMIC utility
- category: data/rules/windows/process_creation
- level: medium
- id: 847d5ff3-8a31-4737-a970-aeae8fe21765

Title: Suspicious Dump64.exe Execution
- description: Detects when a user bypasses Defender by renaming a tool to dump64.exe and placing it in a Visual Studio folder
- category: data/rules/windows/process_creation
- level: high
- id: 129966c9-de17-4334-a123-8b58172e664d

Title: Use of CLIP
- description: Adversaries may collect data stored in the clipboard from users copying information within or between applicati
- category: data/rules/windows/process_creation
- level: low
- id: ddeff553-5233-4ae9-bbab-d64d2bd634be

Title: Mshta JavaScript Execution
- description: Identifies suspicious mshta.exe commands.
- category: data/rules/windows/process_creation
- level: high
- id: 67f113fa-e23d-4271-befa-30113b3e08b1

Title: GALLIUM Artefacts
- description: Detects artefacts associated with activity group GALLIUM - Microsoft Threat Intelligence Center indicators rele
- category: data/rules/windows/process_creation
- level: high
- id: 440a56bf-7873-4439-940a-1c8a671073c2

Title: Suspicious Add User to Remote Desktop Users Group
- description: Detects suspicious command line in which a user gets added to the local Remote Desktop Users group
- category: data/rules/windows/process_creation

- level: high
- id: ffa28e60-bdb1-46e0-9f82-05f7a61cc06e

Title: Suspicious DumpMinitool Usage
- description: Detects suspicious ways to use of a Visual Studio bundled tool named DumpMinitool.exe
- category: data/rules/windows/process_creation
- level: high
- id: eb1c4225-1c23-4241-8dd4-051389fde4ce

Title: Suspicious Process Parents
- description: Detects suspicious parent processes that should not have any children or should only have a single possible chi
- category: data/rules/windows/process_creation
- level: high
- id: cbec226f-63d9-4eca-9f52-dfb6652f24df

Title: Local Accounts Discovery
- description: Local accounts, System Owner/User discovery using operating systems utilities
- category: data/rules/windows/process_creation
- level: low
- id: 502b42de-4306-40b4-9596-6f590c81f073

Title: Redirect Output in CommandLine
- description: Use ">" to redicrect information in commandline
- category: data/rules/windows/process_creation
- level: low
- id: 4f4eaa9f-5ad4-410c-a4be-bc6132b0175a

Title: Network Sniffing
- description: Network sniffing refers to using the network interface on a system to monitor or capture information sent over
- category: data/rules/windows/process_creation
- level: low
- id: ba1f7802-adc7-48b4-9ecb-81e227fddfd5

Title: Possible Applocker Bypass
- description: Detects execution of executables that can be used to bypass Applocker whitelisting
- category: data/rules/windows/process_creation
- level: low
- id: 82a19e3a-2bfe-4a91-8c0d-5d4c98fbb719

Title: Suspicious XOR Encoded PowerShell Command Line
- description: Detects suspicious powershell process which includes bxor command, alternative obfuscation method to b64 encode
- category: data/rules/windows/process_creation
- level: medium
- id: bb780e0c-16cf-4383-8383-1e5471db6cf9

Title: Registry Dump of SAM Creds and Secrets
- description: Adversaries may attempt to extract credential material from the Security Account Manager (SAM) database either
- category: data/rules/windows/process_creation
- level: high
- id: 038cd51c-3ad8-41c5-ba8f-5d1c92f3cc1e

Title: TA505 Dropper Load Pattern
- description: Detects mshta loaded by wmiprvse as parent as used by TA505 malicious documents
- category: data/rules/windows/process_creation
- level: critical
- id: 18cf6cf0-39b0-4c22-9593-e244bdc9a2d4

Title: Copy from Admin Share
- description: Detects a suspicious copy command to or from an Admin share
- category: data/rules/windows/process_creation
- level: high
- id: 855bc8b5-2ae8-402e-a9ed-b889e6df1900

Title: Monitoring Winget For LOLbin Execution
- description: Adversaries can abuse winget to download payloads remotely and execute them without touching disk. Winget will
- category: data/rules/windows/process_creation
- level: medium
- id: 313d6012-51a0-4d93-8dfc-de8553239e25

Title: Suspicious Use of CSharp Interactive Console
- description: Detects the execution of CSharp interactive console by PowerShell
- category: data/rules/windows/process_creation
- level: high
- id: a9e416a8-e613-4f8b-88b8-a7d1d1af2f61

Title: Emotet RunDLL32 Process Creation
- description: Detecting Emotet DLL loading by looking for rundll32.exe processes with command lines ending in ,RunDLL or ,Con
- category: data/rules/windows/process_creation
- level: critical
- id: 54e57ce3-0672-46eb-a402-2c0948d5e3e9

Title: Suspicious Extexport Execution
- description: Extexport.exe loads dll and is execute from other folder the original path
- category: data/rules/windows/process_creation
- level: medium
- id: fb0b815b-f5f6-4f50-970f-ffe21f253f7a

Title: Psexec Accepteula Condition
- description: Detect ed user accept agreement execution in psexec commandline
- category: data/rules/windows/process_creation
- level: medium
- id: 730fc21b-eaff-474b-ad23-90fd265d4988

Title: Suspicious PowerShell IEX Execution Patterns
- description: Detects suspicious ways to run Invoke-Execution using IEX acronym
- category: data/rules/windows/process_creation
- level: high
- id: 09576804-7a05-458e-a817-eb718ca91f54

Title: Parent in Public Folder Suspicious Process
- description: This rule detects suspicious processes with parent images located in the C:\Users\Public folder
- category: data/rules/windows/process_creation
- level: high
- id: 69bd9b97-2be2-41b6-9816-fb08757a4d1a

Title: Maze Ransomware
- description: Detects specific process characteristics of Maze ransomware word document droppers
- category: data/rules/windows/process_creation
- level: critical
- id: 29fd07fc-9cfd-4331-b7fd-cc18dfa21052

Title: Service ImagePath Change with Reg.exe
- description: Adversaries may execute their own malicious payloads by hijacking the Registry entries used by services.

Adversaries may use flaws in the permissions for registry to redirect from the originally specified executable to one that they control, in order to launch their own code at Service start. Windows stores local service configuration information in the Registry under HKLM\SYSTEM\CurrentControlSet\Services

- category: data/rules/windows/process_creation
- level: medium
- id: 9b0b7ac3-6223-47aa-a3fd-e8f211e637db

Title: Webshell Hacking Activity Patterns
- description: Detects certain parent child patterns found in cases in which a webshell is used to perform certain credential
- category: data/rules/windows/process_creation
- level: high
- id: 4ebc877f-4612-45cb-b3a5-8e3834db36c9

Title: Suspicious Msiexec Quiet Install
- description: Adversaries may abuse msiexec.exe to proxy execution of malicious payloads.

Msiexec.exe is the command-line utility for the Windows Installer and is thus commonly associated with executing installation packages (.msi)

- category: data/rules/windows/process_creation
- level: low
- id: 79a87aa6-e4bd-42fc-a5bb-5e6fbdcd62f5

Title: UAC Bypass Using IEInstal - Process
- description: Detects the pattern of UAC Bypass using IEInstal.exe (UACMe 64)
- category: data/rules/windows/process_creation

- level: high
- id: 80fc36aa-945e-4181-89f2-2f907ab6775d

Title: Sysprep on AppData Folder
- description: Detects suspicious sysprep process start with AppData folder as target (as used by Trojan Syndicasec in Thrip r
- category: data/rules/windows/process_creation
- level: medium
- id: d5b9ae7a-e6fc-405e-80ff-2ff9dcc64e7e

Title: Rundll32 InstallScreenSaver Execution
- description: An attacker may execute an application as a SCR File using rundll32.exe desk.cpl,InstallScreenSaver
- category: data/rules/windows/process_creation
- level: medium
- id: 15bd98ea-55f4-4d37-b09a-e7caa0fa2221

Title: Rundll32 Without Parameters
- description: Detects rundll32 execution without parameters as observed when running Metasploit windows/smb/psexec exploit mo
- category: data/rules/windows/process_creation
- level: high
- id: 5bb68627-3198-40ca-b458-49f973db8752

Title: Renamed MegaSync
- description: Detects the execution of a renamed meg.exe of MegaSync during incident response engagements associated with ran
- category: data/rules/windows/process_creation
- level: high
- id: 643bdcac-8b82-49f4-9fd9-25a90b929f3b

Title: UAC Bypass Abusing Winsat Path Parsing - Process
- description: Detects the pattern of UAC Bypass using a path parsing issue in winsat.exe (UACMe 52)
- category: data/rules/windows/process_creation
- level: high
- id: 7a01183d-71a2-46ad-ad5c-acd989ac1793

Title: Suspicious Shells Spawn by Java Utility Keytool
- description: Detects suspicious shell spawn from Java utility keytool process (e.g. adselfservice plus exploitation)
- category: data/rules/windows/process_creation
- level: high
- id: 90fb5e62-ca1f-4e22-b42e-cc521874c938

Title: WMI Remote Command Execution
- description: An adversary might use WMI to execute commands on a remote system
- category: data/rules/windows/process_creation
- level: medium
- id: e42af9df-d90b-4306-b7fb-05c863847ebd

Title: Capture Credentials with Rpcping.exe
- description: Detects using Rpcping.exe to send a RPC test connection to the target server (-s) and force the NTLM hash to be
- category: data/rules/windows/process_creation
- level: medium
- id: 93671f99-04eb-4ab4-a161-70d446a84003

Title: Invoke-Obfuscation Via Use Rundll32
- description: Detects Obfuscated Powershell via use Rundll32 in Scripts
- category: data/rules/windows/process_creation
- level: high
- id: 36c5146c-d127-4f85-8e21-01bf62355d5a

Title: Suspicious Diantz Alternate Data Stream Execution
- description: Compress taget file into a cab file stored in the Alternate Data Stream (ADS) of the target file.
- category: data/rules/windows/process_creation
- level: medium
- id: 6b369ced-4b1d-48f1-b427-fdc0de0790bd

Title: Command Line Execution with Suspicious URL and AppData Strings
- description: Detects a suspicious command line execution that includes an URL and AppData string in the command line paramet
- category: data/rules/windows/process_creation
- level: medium
- id: 1ac8666b-046f-4201-8aba-1951aaec03a3

Title: KrbRelay Hack Tool
- description: Detects the use of KrbRelay, a Kerberos relaying tool
- category: data/rules/windows/process_creation
- level: high
- id: e96253b8-6b3b-4f90-9e59-3b24b99cf9b4

Title: Cabinet File Expansion
- description: Adversaries can use the inbuilt expand utility to decompress cab files as seen in recent Iranian MeteorExpress
- category: data/rules/windows/process_creation
- level: medium
- id: 9f107a84-532c-41af-b005-8d12a607639f

Title: Xwizard DLL Sideloading
- description: Detects the execution of Xwizard tool from the non-default directory which can be used to sideload a custom xwi
- category: data/rules/windows/process_creation
- level: high
- id: 193d5ccd-6f59-40c6-b5b0-8e32d5ddd3d1

Title: Suspicious Service Binary Directory
- description: Detects a service binary running in a suspicious directory
- category: data/rules/windows/process_creation
- level: high
- id: 883faa95-175a-4e22-8181-e5761aeb373c

Title: Ie4uinit Lolbin Use From Invalid Path
- description: Detect use of ie4uinit.exe to execute commands from a specially prepared ie4uinit.inf file from a directory oth
- category: data/rules/windows/process_creation
- level: medium
- id: d3bf399f-b0cf-4250-8bb4-dfc192ab81dc

Title: Base64 Encoded Listing of Shadowcopy
- description: Detects base64 encoded listing Win32_Shadowcopy
- category: data/rules/windows/process_creation
- level: high
- id: 47688f1b-9f51-4656-b013-3cc49a166a36

Title: TrustedPath UAC Bypass Pattern
- description: Detects indicators of a UAC bypass method by mocking directories
- category: data/rules/windows/process_creation
- level: critical
- id: 4ac47ed3-44c2-4b1f-9d51-bf46e8914126

Title: Invoke-Obfuscation Via Stdin
- description: Detects Obfuscated Powershell via Stdin in Scripts
- category: data/rules/windows/process_creation
- level: high
- id: 9c14c9fa-1a63-4a64-8e57-d19280559490

Title: DInject PowerShell Cradle CommandLine Flags
- description: Detects the use of the Dinject PowerShell cradle based on the specific flags
- category: data/rules/windows/process_creation
- level: critical
- id: d78b5d61-187d-44b6-bf02-93486a80de5a

Title: Node Process Executions
- description: Detects the execution of other scripts using the Node executable packaged with Adobe Creative Cloud
- category: data/rules/windows/process_creation
- level: medium
- id: df1f26d3-bea7-4700-9ea2-ad3e990cf90e

Title: UAC Bypass Using PkgMgr and DISM
- description: Detects the pattern of UAC Bypass using pkgmgr.exe and dism.exe (UACMe 23)
- category: data/rules/windows/process_creation
- level: high
- id: a743ceba-c771-4d75-97eb-8a90f7f4844c

Title: Suspicious Program Names
- description: Detects suspicious patterns in program names or folders that are often found in malicious samples or hacktools
- category: data/rules/windows/process_creation

- level: high
- id: efdd8dd5-cee8-4e59-9390-7d4d5e4dd6f6

Title: Suspicious PowerShell Parent Process
- description: Detects a suspicious parents of powershell.exe
- category: data/rules/windows/process_creation
- level: high
- id: 754ed792-634f-40ae-b3bc-e0448d33f695

Title: Ngrok Usage
- description: Detects the use of Ngrok, a utility used for port forwarding and tunneling, often used by threat actors to make
- category: data/rules/windows/process_creation
- level: high
- id: ee37eb7c-a4e7-4cd5-8fa4-efa27f1c3f31

Title: Suspicious NT Resource Kit Auditpol Usage
- description: Threat actors can use an older version of the auditpol binary available inside the NT resource kit to change au
- category: data/rules/windows/process_creation
- level: high
- id: c6c56ada-612b-42d1-9a29-adad3c5c2c1e

Title: Cscript Visual Basic Script Execution
- description: Adversaries may abuse Visual Basic (VB) for execution
- category: data/rules/windows/process_creation
- level: medium
- id: 23250293-eed5-4c39-b57a-841c8933a57d

Title: Malicious Windows Script Components File Execution by TAEF Detection
- description: Windows Test Authoring and Execution Framework (TAEF) framework allows you to run automation by executing tests
- category: data/rules/windows/process_creation
- level: low
- id: 634b00d5-ccc3-4a06-ae3b-0ec8444dd51b

Title: Uninstall Crowdstrike Falcon
- description: Adversaries may disable security tools to avoid possible detection of their tools and activities by uninstallin
- category: data/rules/windows/process_creation
- level: medium
- id: f0f7be61-9cf5-43be-9836-99d6ef448a18

Title: DIT Snapshot Viewer Use
- description: Detects the use of Ditsnap tool. Seems to be a tool for ransomware groups.
- category: data/rules/windows/process_creation
- level: high
- id: d3b70aad-097e-409c-9df2-450f80dc476b

Title: Conti NTDS Exfiltration Command
- description: Detects a command used by conti to exfiltrate NTDS
- category: data/rules/windows/process_creation
- level: high
- id: aa92fd02-09f2-48b0-8a93-864813fb8f41

Title: PurpleSharp Indicator
- description: Detects the execution of the PurpleSharp adversary simulation tool
- category: data/rules/windows/process_creation
- level: critical
- id: ff23ffbc-3378-435e-992f-0624dcf93ab4

Title: Renamed Binary
- description: Detects the execution of a renamed binary often used by attackers or malware leveraging new Sysmon OriginalFile
- category: data/rules/windows/process_creation
- level: medium
- id: 36480ae1-a1cb-4eaa-a0d6-29801d7e9142

Title: Exploit for CVE-2017-0261
- description: Detects Winword starting uncommon sub process FLTLDR.exe as used in exploits for CVE-2017-0261 and CVE-2017-026
- category: data/rules/windows/process_creation
- level: medium
- id: 864403a1-36c9-40a2-a982-4c9a45f7d833

Title: Dridex Process Pattern
- description: Detects typical Dridex process patterns
- category: data/rules/windows/process_creation
- level: critical
- id: e6eb5a96-9e6f-4a18-9cdd-642cfda21c8e

Title: Suspicious ZipExec Execution
- description: ZipExec is a Proof-of-Concept (POC) tool to wrap binary-based tools into a password-protected zip file.
- category: data/rules/windows/process_creation
- level: medium
- id: 90dcf730-1b71-4ae7-9ffc-6fcf62bd0132

Title: Direct Autorun Keys Modification
- description: Detects direct modification of autostart extensibility point (ASEP) in registry using reg.exe.
- category: data/rules/windows/process_creation
- level: medium
- id: 24357373-078f-44ed-9ac4-6d334a668a11

Title: PsExec Tool Execution
- description: Detects PsExec service installation and execution events (service and Sysmon)
- category: data/rules/windows/process_creation
- level: low
- id: fa91cc36-24c9-41ce-b3c8-3bbc3f2f67ba

Title: Query Registry
- description: Adversaries may interact with the Windows Registry to gather information about the system, configuration, and i
- category: data/rules/windows/process_creation
- level: low
- id: 970007b7-ce32-49d0-a4a4-fbef016950bd

Title: Suspicious Diantz Download and Compress Into a CAB File
- description: Download and compress a remote file and store it in a cab file on local machine.
- category: data/rules/windows/process_creation
- level: medium
- id: 185d7418-f250-42d0-b72e-0c8b70661e93

Title: Fsutil Suspicious Invocation
- description: Detects suspicious parameters of fsutil (deleting USN journal, configuring it with small size, etc). Might be u
- category: data/rules/windows/process_creation
- level: high
- id: add64136-62e5-48ea-807e-88638d02df1e

Title: Visual Basic Command Line Compiler Usage
- description: Detects successful code compilation via Visual Basic Command Line Compiler that utilizes Windows Resource to Ob
- category: data/rules/windows/process_creation
- level: high
- id: 7b10f171-7f04-47c7-9fa2-5be43c76e535

Title: ProtocolHandler.exe Downloaded Suspicious File
- description: Emulates attack via documents through protocol handler in Microsoft Office. On successful execution you should
- category: data/rules/windows/process_creation
- level: medium
- id: 104cdb48-a7a8-4ca7-a453-32942c6e5dcb

Title: Shadow Copies Creation Using Operating Systems Utilities
- description: Shadow Copies creation using operating systems utilities, possible credential access
- category: data/rules/windows/process_creation
- level: medium
- id: b17ea6f7-6e90-447e-a799-e6c0a493d6ce

Title: Process Start From Suspicious Folder
- description: Detects process start from rare or uncommon folders like temporary folder or folders that usually don't contain
- category: data/rules/windows/process_creation
- level: low
- id: dca91cfd-d7ab-4c66-8da7-ee57d487b35b

Title: MSHTA Spawning Windows Shell
- description: Detects a Windows command line executable started from MSHTA
- category: data/rules/windows/process_creation

- level: high
- id: 03cc0c25-389f-4bf8-b48d-11878079f1ca

Title: Renamed ZOHO Dctask64
- description: Detects a renamed dctask64.exe used for process injection, command execution, process creation with a signed bi
- category: data/rules/windows/process_creation
- level: high
- id: 340a090b-c4e9-412e-bb36-b4b16fe96f9b

Title: Suspicious Characters in CommandLine
- description: Detects suspicious characters in the command line, which could be a sign of obfuscation
- category: data/rules/windows/process_creation
- level: high
- id: 2c0d2d7b-30d6-4d14-9751-7b9113042ab9

Title: PowerShell Encoded Character Syntax
- description: Detects suspicious encoded character syntax often used for defense evasion
- category: data/rules/windows/process_creation
- level: high
- id: e312efd0-35a1-407f-8439-b8d434b438a6

Title: Exports Critical Registry Keys To a File
- description: Detects the export of a crital Registry key to a file.
- category: data/rules/windows/process_creation
- level: high
- id: 82880171-b475-4201-b811-e9c826cd5eaa

Title: UAC Bypass Using ComputerDefaults
- description: Detects the pattern of UAC Bypass using computerdefaults.exe (UACMe 59)
- category: data/rules/windows/process_creation
- level: high
- id: 3c05e90d-7eba-4324-9972-5d7f711a60a8

Title: SQL Client Tools PowerShell Session Detection
- description: This rule detects execution of a PowerShell code through the sqltoolsps.exe utility, which is included in the s
- category: data/rules/windows/process_creation
- level: medium
- id: a746c9b8-a2fb-4ee5-a428-92bee9e99060

Title: Abusing Print Executable
- description: Attackers can use print.exe for remote file copy
- category: data/rules/windows/process_creation
- level: medium
- id: bafac3d6-7de9-4dd9-8874-4a1194b493ed

Title: Suspicious Certutil Command
- description: Detects a suspicious Microsoft certutil execution with sub commands like 'decode' sub command, which is sometim
- category: data/rules/windows/process_creation
- level: high
- id: e011a729-98a6-4139-b5c4-bf6f6dd8239a

Title: Rubeus Hack Tool
- description: Detects command line parameters used by Rubeus hack tool
- category: data/rules/windows/process_creation
- level: critical
- id: 7ec2c172-dceb-4c10-92c9-87c1881b7e18

Title: GfxDownloadWrapper.exe Downloads File from Suspicious URL
- description: Detects when GfxDownloadWrapper.exe downloads file from non standard URL
- category: data/rules/windows/process_creation
- level: medium
- id: eee00933-a761-4cd0-be70-c42fe91731e7

Title: Writing Of Malicious Files To The Fonts Folder
- description: Monitors for the hiding possible malicious files in the C:\Windows\Fonts\ location. This folder doesn't require
- category: data/rules/windows/process_creation
- level: medium
- id: ae9b0bd7-8888-4606-b444-0ed7410cb728

Title: NodejsTools PressAnyKey Lolbin
- description: Detects a certain command line flag combination used by Microsoft.NodejsTools.PressAnyKey.exe that can be used
- category: data/rules/windows/process_creation
- level: high
- id: a20391f8-76fb-437b-abc0-dba2df1952c6

Title: Suspicious Plink Remote Forwarding
- description: Detects suspicious Plink tunnel remote forarding to a local port
- category: data/rules/windows/process_creation
- level: high
- id: 48a61b29-389f-4032-b317-b30de6b95314

Title: Command Line Path Traversal Evasion
- description: Detects the attempt to evade or obfuscate the executed command on the CommandLine using bogus path traversal
- category: data/rules/windows/process_creation
- level: high
- id: 1327381e-6ab0-4f38-b583-4c1b8346a56b

Title: Netsh Port Forwarding
- description: Detects netsh commands that configure a port forwarding (PortProxy)
- category: data/rules/windows/process_creation
- level: medium
- id: 322ed9ec-fcab-4f67-9a34-e7c6aef43614

Title: Ryuk Ransomware
- description: Detects Ryuk ransomware activity
- category: data/rules/windows/process_creation
- level: critical
- id: c37510b8-2107-4b78-aa32-72f251e7a844

Title: Process Access via TrolleyExpress Exclusion
- description: Detects a possible process memory dump that uses the white-listed Citrix TrolleyExpress.exe filename as a way t
- category: data/rules/windows/process_creation
- level: high
- id: 4c0aaedc-154c-4427-ada0-d80ef9c9deb6

Title: Suspicious AdFind Enumerate
- description: Detects the execution of a AdFind for enumeration
- category: data/rules/windows/process_creation
- level: medium
- id: 455b9d50-15a1-4b99-853f-8d37655a4c1b

Title: Disabled IE Security Features
- description: Detects command lines that indicate unwanted modifications to registry keys that disable important Internet Exp
- category: data/rules/windows/process_creation
- level: high
- id: fb50eb7a-5ab1-43ae-bcc9-091818cb8424

Title: PowerShell Base64 Encoded Shellcode
- description: Detects Base64 encoded Shellcode
- category: data/rules/windows/process_creation
- level: critical
- id: 2d117e49-e626-4c7c-bd1f-c3c0147774c8

Title: Lazarus Loaders
- description: Detects different loaders as described in various threat reports on Lazarus group activity
- category: data/rules/windows/process_creation
- level: critical
- id: 7b49c990-4a9a-4e65-ba95-47c9cc448f6e

Title: AnyDesk Silent Installation
- description: AnyDesk Remote Desktop silent installation can be used by attacker to gain remote access.
- category: data/rules/windows/process_creation
- level: high
- id: 114e7f1c-f137-48c8-8f54-3088c24ce4b9

Title: Custom Class Execution via Xwizard
- description: Detects the execution of Xwizard tool with specific arguments which utilized to run custom class properties.
- category: data/rules/windows/process_creation

- level: medium
- id: 53d4bb30-3f36-4e8a-b078-69d36c4a79ff

Title: Suspicious Compression Tool Parameters
- description: Detects suspicious command line arguments of common data compression tools
- category: data/rules/windows/process_creation
- level: high
- id: 27a72a60-7e5e-47b1-9d17-909c9abafdcd

Title: MsiExec Web Install
- description: Detects suspicious msiexec process starts with web addresses as parameter
- category: data/rules/windows/process_creation
- level: medium
- id: f7b5f842-a6af-4da5-9e95-e32478f3cd2f

Title: Execution of Powershell Script in Public Folder
- description: This rule detects execution of PowerShell scripts located in the C:\Users\Public folder
- category: data/rules/windows/process_creation
- level: high
- id: fb9d3ff7-7348-46ab-af8c-b55f5fbf39b4

Title: Possible Shim Database Persistence via sdbinst.exe
- description: Detects installation of a new shim using sdbinst.exe. A shim can be used to load malicious DLLs into applicatio
- category: data/rules/windows/process_creation
- level: high
- id: 517490a7-115a-48c6-8862-1a481504d5a8

Title: Exploited CVE-2020-10189 Zoho ManageEngine
- description: Detects the exploitation of Zoho ManageEngine Desktop Central Java Deserialization vulnerability reported as CV
- category: data/rules/windows/process_creation
- level: critical
- id: 846b866e-2a57-46ee-8e16-85fa92759be7

Title: File Download with Headless Browser
- description: This is an unusual method to download files. It starts a browser headless and downloads a file from a location.
- category: data/rules/windows/process_creation
- level: high
- id: 0e8cfe08-02c9-4815-a2f8-0d157b7ed33e

Title: Compress Data and Lock With Password for Exfiltration With WINZIP
- description: An adversary may compress or encrypt data that is collected prior to exfiltration using 3rd party utilities
- category: data/rules/windows/process_creation
- level: medium
- id: e2e80da2-8c66-4e00-ae3c-2eebd29f6b6d

Title: Suspicious Double Extension
- description: Detects suspicious use of an .exe extension after a non-executable file extension like .pdf.exe, a set of space
- category: data/rules/windows/process_creation
- level: critical
- id: 1cdd9a09-06c9-4769-99ff-626e2b3991b8

Title: Domain Trust Discovery
- description: Identifies execution of nltest.exe and dsquery.exe for domain trust discovery. This technique is used by attack
- category: data/rules/windows/process_creation
- level: medium
- id: 3bad990e-4848-4a78-9530-b427d854aac0

Title: Suspicious Msiexec Execute Arbitrary DLL
- description: Adversaries may abuse msiexec.exe to proxy execution of malicious payloads.

Msiexec.exe is the command-line utility for the Windows Installer and is thus commonly associated with executing installation packages (.msi)

- category: data/rules/windows/process_creation
- level: medium
- id: 6f4191bb-912b-48a8-9ce7-682769541e6d

Title: Monitoring For Persistence Via BITS
- description: BITS will allow you to schedule a command to execute after a successful download to notify you that the job is
- category: data/rules/windows/process_creation

- level: medium
- id: b9cbbc17-d00d-4e3d-a827-b06d03d2380d

Title: WSF/JSE/JS/VBA/VBE File Execution
- description: Detects suspicious file execution by wscript and cscript
- category: data/rules/windows/process_creation
- level: medium
- id: 1e33157c-53b1-41ad-bbcc-780b80b58288

Title: Greenbug Campaign Indicators
- description: Detects tools and process executions as observed in a Greenbug campaign in May 2020
- category: data/rules/windows/process_creation
- level: critical
- id: 3711eee4-a808-4849-8a14-faf733da3612

Title: Procdump Usage
- description: Detects uses of the SysInternals Procdump utility
- category: data/rules/windows/process_creation
- level: medium
- id: 2e65275c-8288-4ab4-aeb7-6274f58b6b20

Title: Renamed PowerShell
- description: Detects the execution of a renamed PowerShell often used by attackers or malware
- category: data/rules/windows/process_creation
- level: critical
- id: d178a2d7-129a-4ba4-8ee6-d6e1fecd5d20

Title: Modification Of Existing Services For Persistence
- description: Detects modification of an existing service on a compromised host in order to execute an arbitrary payload when
- category: data/rules/windows/process_creation
- level: medium
- id: 38879043-7e1e-47a9-8d46-6bec88e201df

Title: Koadic Execution
- description: Detects command line parameters used by Koadic hack tool
- category: data/rules/windows/process_creation
- level: high
- id: 5cddf373-ef00-4112-ad72-960ac29bac34

Title: Impacket Tool Execution
- description: Detects the execution of different compiled Windows binaries of the impacket toolset (based on names or part of
- category: data/rules/windows/process_creation
- level: high
- id: 4627c6ae-6899-46e2-aa0c-6ebcb1becd19

Title: Execution via CL_Invocation.ps1
- description: Detects Execution via SyncInvoke in CL_Invocation.ps1 module
- category: data/rules/windows/process_creation
- level: high
- id: a0459f02-ac51-4c09-b511-b8c9203fc429

Title: PowerShell DownloadFile
- description: Detects the execution of powershell, a WebClient object creation and the invocation of DownloadFile in a single
- category: data/rules/windows/process_creation
- level: high
- id: 8f70ac5f-1f6f-4f8e-b454-db19561216c5

Title: Suspicious Splwow64 Without Params
- description: Detects suspicious Splwow64.exe process without any command line parameters
- category: data/rules/windows/process_creation
- level: high
- id: 1f1a8509-2cbb-44f5-8751-8e1571518ce2

Title: Conti Backup Database
- description: Detects a command used by conti to dump database
- category: data/rules/windows/process_creation
- level: high
- id: 2f47f1fd-0901-466e-a770-3b7092834a1b

Title: Scheduled Task WScript VBScript
- description: Detects specific process parameters as used by ACTINIUM scheduled task persistence creation.
- category: data/rules/windows/process_creation
- level: high
- id: e1118a8f-82f5-44b3-bb6b-8a284e5df602

Title: Suspicious Script Execution From Temp Folder
- description: Detects a suspicious script executions from temporary folder
- category: data/rules/windows/process_creation
- level: high
- id: a6a39bdb-935c-4f0a-ab77-35f4bbf44d33

Title: Finger.exe Suspicious Invocation
- description: Detects suspicious aged finger.exe tool execution often used in malware attacks nowadays
- category: data/rules/windows/process_creation
- level: high
- id: af491bca-e752-4b44-9c86-df5680533dbc

Title: Reconnaissance Activity with Net Command
- description: Detects a set of commands often used in recon stages by different attack groups
- category: data/rules/windows/process_creation
- level: medium
- id: 2887e914-ce96-435f-8105-593937e90757

Title: Suspicious Execution of Hostname
- description: Use of hostname to get information
- category: data/rules/windows/process_creation
- level: low
- id: 7be5fb68-f9ef-476d-8b51-0256ebece19e

Title: False Sysinternals Suite Tools
- description: Rename as a legitim Sysinternals Suite tools to evade detection
- category: data/rules/windows/process_creation
- level: medium
- id: 7cce6fc8-a07f-4d84-a53e-96e1879843c9

Title: Ryuk Ransomware
- description: Detects Ryuk Ransomware command lines
- category: data/rules/windows/process_creation
- level: critical
- id: 0acaad27-9f02-4136-a243-c357202edd74

Title: Invocation of Active Directory Diagnostic Tool (ntdsutil.exe)
- description: Detects execution of ntdsutil.exe, which can be used for various attacks against the NTDS database (NTDS.DIT)
- category: data/rules/windows/process_creation
- level: medium
- id: 2afafd61-6aae-4df4-baed-139fa1f4c345

Title: Accesschk Usage After Privilege Escalation
- description: Accesschk is an access and privilege audit tool developed by SysInternal and often being used by attacker to ve
- category: data/rules/windows/process_creation
- level: high
- id: c625d754-6a3d-4f65-9c9a-536aea960d37

Title: DevInit Lolbin Download
- description: Detects a certain command line flag combination used by devinit.exe lolbin to download arbitrary MSI packages o
- category: data/rules/windows/process_creation
- level: high
- id: 90d50722-0483-4065-8e35-57efaadd354d

Title: Netsh RDP Port Opening
- description: Detects netsh commands that opens the port 3389 used for RDP, used in Sarwent Malware
- category: data/rules/windows/process_creation
- level: high
- id: 01aeb693-138d-49d2-9403-c4f52d7d3d62

Title: Disabled Volume Snapshots
- description: Detects commands that temporarily turn off Volume Snapshots
- category: data/rules/windows/process_creation

- level: high
- id: dee4af55-1f22-4e1d-a9d2-4bdc7ecb472a

Title: Powershell AMSI Bypass via .NET Reflection
- description: Detects Request to amsiInitFailed that can be used to disable AMSI Scanning
- category: data/rules/windows/process_creation
- level: high
- id: 30edb182-aa75-42c0-b0a9-e998bb29067c

Title: PowerShell Script Run in AppData
- description: Detects a suspicious command line execution that invokes PowerShell with reference to an AppData folder
- category: data/rules/windows/process_creation
- level: medium
- id: ac175779-025a-4f12-98b0-acdaeb77ea85

Title: Covenant Launcher Indicators
- description: Detects suspicious command lines used in Covenant luanchers
- category: data/rules/windows/process_creation
- level: high
- id: c260b6db-48ba-4b4a-a76f-2f67644e99d2

Title: RdrLeakDiag Process Dump
- description: Detects uses of the rdrleakdiag.exe LOLOBIN utility to dump process memory
- category: data/rules/windows/process_creation
- level: high
- id: 6355a919-2e97-4285-a673-74645566340d

Title: Suspicious Schtasks Execution AppData Folder
- description: Detects the creation of a schtask that executes a file from C:\Users\<USER>\AppData\Local
- category: data/rules/windows/process_creation
- level: high
- id: c5c00f49-b3f9-45a6-997e-cfdecc6e1967

Title: Trickbot Malware Recon Activity
- description: Trickbot enumerates domain/network topology and executes certain commands automatically every few minutes. This
- category: data/rules/windows/process_creation
- level: critical
- id: 410ad193-a728-4107-bc79-4419789fcbf8

Title: UAC Bypass Using NTFS Reparse Point - Process
- description: Detects the pattern of UAC Bypass using NTFS reparse point and wusa.exe DLL hijacking (UACMe 36)
- category: data/rules/windows/process_creation
- level: high
- id: 39ed3c80-e6a1-431b-9df3-911ac53d08a7

Title: Remote Desktop Protocol Use Mstsc
- description: Adversaries may use Valid Accounts to log into a computer using the Remote Desktop Protocol (RDP). The adversar
- category: data/rules/windows/process_creation
- level: medium
- id: 954f0af7-62dd-418f-b3df-a84bc2c7a774

Title: Suspicious UltraVNC Execution
- description: Detects suspicious UltraVNC command line flag combination that indicate a auto reconnect upon execution, e.g. s
- category: data/rules/windows/process_creation
- level: high
- id: 871b9555-69ca-4993-99d3-35a59f9f3599

Title: Modifies the Registry From a File
- description: Detects the execution of regini.exe which can be used to modify registry keys, the changes are imported from on
- category: data/rules/windows/process_creation
- level: low
- id: 5f60740a-f57b-4e76-82a1-15b6ff2cb134

Title: Net.exe Execution
- description: Detects execution of Net.exe, whether suspicious or benign.
- category: data/rules/windows/process_creation
- level: low
- id: 183e7ea8-ac4b-4c23-9aec-b3dac4e401ac

Title: Execution from Suspicious Folder
- description: Detects a suspicious execution from an uncommon folder
- category: data/rules/windows/process_creation
- level: high
- id: 3dfd06d2-eaf4-4532-9555-68aca59f57c4

Title: High Integrity Sdclt Process
- description: A General detection for sdclt being spawned as an elevated process. This could be an indicator of sdclt being u
- category: data/rules/windows/process_creation
- level: medium
- id: 40f9af16-589d-4984-b78d-8c2aec023197

Title: Suspicious Execution of Taskkill
- description: Adversaries may stop services or processes in order to conduct Data Destruction or Data Encrypted for Impact on
- category: data/rules/windows/process_creation
- level: low
- id: 86085955-ea48-42a2-9dd3-85d4c36b167d

Title: Scheduled Task Executing Powershell Encoded Payload from Registry
- description: Detects the creation of a schtask that executes a base64 encoded payload stored in the Windows Registry using P
- category: data/rules/windows/process_creation
- level: high
- id: c4eeeeae-89f4-43a7-8b48-8d1bdfa66c78

Title: Always Install Elevated MSI Spawned Cmd And Powershell
- description: This rule looks for Windows Installer service (msiexec.exe) spawned command line and/or powershell
- category: data/rules/windows/process_creation
- level: medium
- id: 1e53dd56-8d83-4eb4-a43e-b790a05510aa

Title: Zip A Folder With PowerShell For Staging In Temp
- description: Use living off the land tools to zip a file and stage it in the Windows temporary folder for later exfiltration
- category: data/rules/windows/process_creation
- level: medium
- id: 85a8e5ba-bd03-4bfb-bbfa-a4409a8f8b98

Title: Sofacy Trojan Loader Activity
- description: Detects Trojan loader activity as used by APT28
- category: data/rules/windows/process_creation
- level: critical
- id: ba778144-5e3d-40cf-8af9-e28fb1df1e20

Title: KrbRelayUp Hack Tool
- description: Detects KrbRelayUp used to perform a universal no-fix local privilege escalation in windows domain environments
- category: data/rules/windows/process_creation
- level: high
- id: 12827a56-61a4-476a-a9cb-f3068f191073

Title: Suspicious WebDav Client Execution
- description: A General detection for svchost.exe spawning rundll32.exe with command arguments like C:\windows\system32\davcl
- category: data/rules/windows/process_creation
- level: medium
- id: 2dbd9d3d-9e27-42a8-b8df-f13825c6c3d5

Title: Discovery of a System Time
- description: Identifies use of various commands to query a systems time. This technique may be used before executing a sched
- category: data/rules/windows/process_creation
- level: low
- id: b243b280-65fe-48df-ba07-6ddea7646427

Title: MpiExec Lolbin
- description: Detects a certain command line flag combination used by mpiexec.exe LOLBIN from HPC pack that can be used to ex
- category: data/rules/windows/process_creation
- level: high
- id: 729ce0ea-5d8f-4769-9762-e35de441586d

Title: Suspicious GrpConv Execution
- description: Detects the suspicious execution of a utility to convert Windows 3.x .grp files or for persistence purposes by
- category: data/rules/windows/process_creation

- level: high
- id: f14e169e-9978-4c69-acb3-1cff8200bc36

Title: Root Certificate Installed
- description: Adversaries may install a root certificate on a compromised system to avoid warnings when connecting to adversa
- category: data/rules/windows/process_creation
- level: medium
- id: 46591fae-7a4c-46ea-aec3-dff5e6d785dc

Title: AdFind Usage Detection
- description: AdFind continues to be seen across majority of breaches. It is used to domain trust discovery to plan out subse
- category: data/rules/windows/process_creation
- level: high
- id: 9a132afa-654e-11eb-ae93-0242ac130002

Title: Findstr Launching .lnk File
- description: Detects usage of findstr to identify and execute a lnk file as seen within the HHS redirect attack
- category: data/rules/windows/process_creation
- level: medium
- id: 33339be3-148b-4e16-af56-ad16ec6c7e7b

Title: Application Executed Non-Executable Extension
- description: Detects the execution of rundll32 with a command line that doesn't contain a .dll file
- category: data/rules/windows/process_creation
- level: high
- id: c3a99af4-35a9-4668-879e-c09aeb4f2bdf

Title: Suspicious Process Patterns NTDS.DIT Exfil
- description: Detects suspicious process patterns used in NTDS.DIT exfiltration
- category: data/rules/windows/process_creation
- level: high
- id: 8bc64091-6875-4881-aaf9-7bd25b5dda08

Title: Suspicious Reg Add Open Command
- description: Threat actors performed dumping of SAM, SECURITY and SYSTEM registry hives using DelegateExecute key
- category: data/rules/windows/process_creation
- level: medium
- id: dd3ee8cc-f751-41c9-ba53-5a32ed47e563

Title: Suspicious RazerInstaller Explorer Subprocess
- description: Detects a explorer.exe sub process of the RazerInstaller software which can be invoked from the installer to se
- category: data/rules/windows/process_creation
- level: high
- id: a4eaf250-7dc1-4842-862a-5e71cd59a167

Title: Invoke-Obfuscation CLIP+ Launcher
- description: Detects Obfuscated use of Clip.exe to execute PowerShell
- category: data/rules/windows/process_creation
- level: high
- id: b222df08-0e07-11eb-adc1-0242ac120002

Title: Suspicious Regsvr32 HTTP IP Pattern
- description: Detects a certain command line flag combination used by regsvr32 when used to download and register a DLL from
- category: data/rules/windows/process_creation
- level: high
- id: 2dd2c217-bf68-437a-b57c-fe9fd01d5de8

Title: Suspicious PowerShell Command Line
- description: Detects the PowerShell command lines with special characters
- category: data/rules/windows/process_creation
- level: high
- id: d7bcd677-645d-4691-a8d4-7a5602b780d1

Title: Dism Remove Online Package
- description: Deployment Image Servicing and Management tool. DISM is used to enumerate, install, uninstall, configure, and u
- category: data/rules/windows/process_creation
- level: medium
- id: 43e32da2-fdd0-4156-90de-50dfd62636f9

Title: Suspicious MsiExec Embedding Parent
- description: Adversaries may abuse msiexec.exe to proxy the execution of malicious payloads
- category: data/rules/windows/process_creation
- level: medium
- id: 4a2a2c3e-209f-4d01-b513-4155a540b469

Title: Exploit for CVE-2017-8759
- description: Detects Winword starting uncommon sub process csc.exe as used in exploits for CVE-2017-8759
- category: data/rules/windows/process_creation
- level: critical
- id: fdd84c68-a1f6-47c9-9477-920584f94905

Title: Execution via Diskshadow.exe
- description: Detects using Diskshadow.exe to execute arbitrary code in text file
- category: data/rules/windows/process_creation
- level: high
- id: 0c2f8629-7129-4a8a-9897-7e0768f13ff2

Title: Use Radmin Viewer Utility
- description: An adversary may use Radmin Viewer Utility to remotely control Windows device
- category: data/rules/windows/process_creation
- level: high
- id: 5817e76f-4804-41e6-8f1d-5fa0b3ecae2d

Title: Registry Parse with Pypykatz
- description: Adversaries may attempt to extract credential material from the Security Account Manager (SAM) database either
- category: data/rules/windows/process_creation
- level: high
- id: a29808fd-ef50-49ff-9c7a-59a9b040b404

Title: ZxShell Malware
- description: Detects a ZxShell start by the called and well-known function name
- category: data/rules/windows/process_creation
- level: critical
- id: f0b70adb-0075-43b0-9745-e82a1c608fcc

Title: CrackMapExec Command Line Flags
- description: This rule detect common flag combinations used by CrackMapExec in order to detect its use even if the binary ha
- category: data/rules/windows/process_creation
- level: high
- id: 42a993dd-bb3e-48c8-b372-4d6684c4106c

Title: ScreenConnect Backstage Mode Anomaly
- description: Detects suspicious sub processes started by the ScreenConnect client service, which indicates the use of the so
- category: data/rules/windows/process_creation
- level: high
- id: 7b582f1a-b318-4c6a-bf4e-66fe49bf55a5

Title: CobaltStrike Load by Rundll32
- description: Rundll32 can be use by Cobalt Strike with StartW function to load DLLs from the command line.
- category: data/rules/windows/process_creation
- level: critical
- id: ae9c6a7c-9521-42a6-915e-5aaa8689d529

Title: Execution in Webserver Root Folder
- description: Detects a suspicious program execution in a web service root folder (filter out false positives)
- category: data/rules/windows/process_creation
- level: medium
- id: 35efb964-e6a5-47ad-bbcd-19661854018d

Title: Abusing IEExec To Download Payloads
- description: Detects execution of the IEExec utility to download payloads
- category: data/rules/windows/process_creation
- level: high
- id: 9801abb8-e297-4dbf-9fbd-57dde0e830ad

Title: Suspicious Download from Office Domain
- description: Detects suspicious ways to download files from Microsoft domains that are used to store attachments in Emails o
- category: data/rules/windows/process_creation

- level: high
- id: 00d49ed5-4491-4271-a8db-650a4ef6f8c1

Title: DumpMinitool Usage
- description: Detects the use of a Visual Studio bundled tool named DumpMinitool.exe
- category: data/rules/windows/process_creation
- level: medium
- id: dee0a7a3-f200-4112-a99b-952196d81e42

Title: New Lolbin Process by Office Applications
- description: This rule will monitor any office apps that spins up a new LOLBin process. This activity is pretty suspicious a
- category: data/rules/windows/process_creation
- level: high
- id: 23daeb52-e6eb-493c-8607-c4f0246cb7d8

Title: Shells Spawn by Java
- description: Detects shell spawn from Java host process, which could a maintenance task or some kind of exploitation (e.g. l
- category: data/rules/windows/process_creation
- level: medium
- id: dff1e1cc-d3fd-47c8-bfc2-aeb878a754c0

Title: Detect Virtualbox Driver Installation OR Starting Of VMs
- description: Adversaries can carry out malicious operations using a virtual instance to avoid detection. This rule is built
- category: data/rules/windows/process_creation
- level: low
- id: bab049ca-7471-4828-9024-38279a4c04da

Title: CreateDump Process Dump
- description: Detects uses of the createdump.exe LOLOBIN utility to dump process memory
- category: data/rules/windows/process_creation
- level: high
- id: 515c8be5-e5df-4c5e-8f6d-a4a2f05e4b48

Title: Invoke-Obfuscation VAR+ Launcher
- description: Detects Obfuscated use of Environment Variables to execute PowerShell
- category: data/rules/windows/process_creation
- level: high
- id: 27aec9c9-dbb0-4939-8422-1742242471d0

Title: Suspicious Netsh DLL Persistence
- description: Detects persitence via netsh helper
- category: data/rules/windows/process_creation
- level: high
- id: 56321594-9087-49d9-bf10-524fe8479452

Title: Suspicious Reg Add BitLocker
- description: Suspicious add key for BitLocker
- category: data/rules/windows/process_creation
- level: medium
- id: 0e0255bf-2548-47b8-9582-c0955c9283f5

Title: SecurityXploded Tool
- description: Detects the execution of SecurityXploded Tools
- category: data/rules/windows/process_creation
- level: critical
- id: 7679d464-4f74-45e2-9e01-ac66c5eb041a

Title: Sensitive Registry Access via Volume Shadow Copy
- description: Detects a command that accesses password storing registry hives via volume shadow backups
- category: data/rules/windows/process_creation
- level: medium
- id: f57f8d16-1f39-4dcb-a604-6c73d9b54b3d

Title: Encoded IEX
- description: Detects a base64 encoded IEX command string in a process command line
- category: data/rules/windows/process_creation
- level: critical
- id: 88f680b8-070e-402c-ae11-d2914f2257f1

```
Title: Invoke-Obfuscation Obfuscated IEX Invocation
- description: Detects all variations of obfuscated powershell IEX invocation code generated by Invoke-Obfuscation framework f
- category: data/rules/windows/process_creation
- level: high
- id: 4bf943c6-5146-4273-98dd-e958fd1e3abf

Title: Use of ScreenConnect Remote Access Software
- description: An adversary may use legitimate desktop support and remote access software, such as Team Viewer, Go2Assist, Log
```

These services are commonly used as legitimate technical support software, and may be allowed by application control within a target environment. Remote access tools like VNC, Ammyy, and Teamviewer are used frequently when compared with other legitimate software commonly used by adversaries. (Citation: Symantec Living off the Land)

```
- category: data/rules/windows/process_creation
- level: medium
- id: 57bff678-25d1-4d6c-8211-8ca106d12053

Title: Operation Wocao Activity
- description: Detects activity mentioned in Operation Wocao report
- category: data/rules/windows/process_creation
- level: high
- id: 1cfac73c-be78-4f9a-9b08-5bde0c3953ab

Title: Esentutl Gather Credentials
- description: Conti recommendation to its affiliates to use esentutl to access NTDS dumped file. Trickbot also uses this util
- category: data/rules/windows/process_creation
- level: medium
- id: 7df1713a-1a5b-4a4b-a071-dc83b144a101

Title: Uninstall Sysinternals Sysmon
- description: Detects the uninstallation of Sysinternals Sysmon, which could be the result of legitimate administration or a
- category: data/rules/windows/process_creation
- level: high
- id: 6a5f68d1-c4b5-46b9-94ee-5324892ea939

Title: Suspicious Use of PsLogList
- description: Threat actors can use the PsLogList utility to dump event log in order to extract admin accounts and perform ac
- category: data/rules/windows/process_creation
- level: medium
- id: aae1243f-d8af-40d8-ab20-33fc6d0c55bc

Title: Use of Anydesk Remote Access Software
- description: An adversary may use legitimate desktop support and remote access software, such as Team Viewer, Go2Assist, Log
```

These services are commonly used as legitimate technical support software, and may be allowed by application control within a target environment. Remote access tools like VNC, Ammyy, and Teamviewer are used frequently when compared with other legitimate software commonly used by adversaries. (Citation: Symantec Living off the Land)

```
- category: data/rules/windows/process_creation
- level: medium
- id: b52e84a3-029e-4529-b09b-71d19dd27e94

Title: Suspicious Bitstransfer via PowerShell
- description: Detects transferring files from system on a server bitstransfer Powershell cmdlets
- category: data/rules/windows/process_creation
- level: medium
- id: cd5c8085-4070-4e22-908d-a5b3342deb74

Title: Run from a Zip File
- description: Payloads may be compressed, archived, or encrypted in order to avoid detection
- category: data/rules/windows/process_creation
- level: medium
- id: 1a70042a-6622-4a2b-8958-267625349abf

Title: Indirect Command Execution
- description: Detect indirect command execution via Program Compatibility Assistant (pcalua.exe or forfiles.exe).
- category: data/rules/windows/process_creation
- level: low
- id: fa47597e-90e9-41cd-ab72-c3b74cfb0d02
```

Title: Suspicious Reconnaissance Activity
- description: Detects suspicious command line activity on Windows systems
- category: data/rules/windows/process_creation
- level: medium
- id: d95de845-b83c-4a9a-8a6a-4fc802ebf6c0

Title: Password Cracking with Hashcat
- description: Execute Hashcat.exe with provided SAM file from registry of Windows and Password list to crack against
- category: data/rules/windows/process_creation
- level: critical
- id: 39b31e81-5f5f-4898-9c0e-2160cfc0f9bf

Title: Harvesting of Wifi Credentials Using netsh.exe
- description: Detect the harvesting of wifi credentials using netsh.exe
- category: data/rules/windows/process_creation
- level: medium
- id: 42b1a5b8-353f-4f10-b256-39de4467faff

Title: Automated Collection Command Prompt
- description: Once established within a system or network, an adversary may use automated techniques for collecting internal
- category: data/rules/windows/process_creation
- level: medium
- id: f576a613-2392-4067-9d1a-9345fb58d8d1

Title: Suspicious DIR Execution
- description: Use dir to collect information
- category: data/rules/windows/process_creation
- level: low
- id: 7c9340a9-e2ee-4e43-94c5-c54ebbea1006

Title: ADCSPwn Hack Tool
- description: Detects command line parameters used by ADCSPwn, a tool to escalate privileges in an active directory network b
- category: data/rules/windows/process_creation
- level: critical
- id: cd8c163e-a19b-402e-bdd5-419ff5859f12

Title: Use of TTDInject.exe
- description: Detects the executiob of TTDInject.exe, which is used by Windows 10 v1809 and newer to debug time travel (under
- category: data/rules/windows/process_creation
- level: medium
- id: b27077d6-23e6-45d2-81a0-e2b356eea5fd

Title: Formbook Process Creation
- description: Detects Formbook like process executions that inject code into a set of files in the System32 folder, which exe
- category: data/rules/windows/process_creation
- level: critical
- id: 032f5fb3-d959-41a5-9263-4173c802dc2b

Title: Suspicious Eventlog Clear or Configuration Using Wevtutil
- description: Detects clearing or configuration of eventlogs using wevtutil, powershell and wmic. Might be used by ransomware
- category: data/rules/windows/process_creation
- level: high
- id: cc36992a-4671-4f21-a91d-6c2b72a2edf5

Title: EvilNum Golden Chickens Deployment via OCX Files
- description: Detects Golden Chickens deployment method as used by Evilnum in report published in July 2020
- category: data/rules/windows/process_creation
- level: critical
- id: 8acf3cfa-1e8c-4099-83de-a0c4038e18f0

Title: Malicious Payload Download via Office Binaries
- description: Downloads payload from remote server
- category: data/rules/windows/process_creation
- level: high
- id: 0c79148b-118e-472b-bdb7-9b57b444cc19

Title: Powershell Used To Disable Windows Defender AV Security Monitoring
- description: Detects attackers attempting to disable Windows Defender using Powershell
- category: data/rules/windows/process_creation

- level: high
- id: a7ee1722-c3c5-aeff-3212-c777e4733217

Title: Possible SPN Enumeration
- description: Detects Service Principal Name Enumeration used for Kerberoasting
- category: data/rules/windows/process_creation
- level: medium
- id: 1eeed653-dbc8-4187-ad0c-eeebb20e6599

Title: Lazarus Activity
- description: Detects different process creation events as described in various threat reports on Lazarus group activity
- category: data/rules/windows/process_creation
- level: critical
- id: 24c4d154-05a4-4b99-b57d-9b977472443a

Title: Whoami Execution
- description: Detects the execution of whoami, which is often used by attackers after exploitation / privilege escalation but
- category: data/rules/windows/process_creation
- level: medium
- id: e28a5a99-da44-436d-b7a0-2afc20a5f413

Title: Hidden Powershell in Link File Pattern
- description: Detects events that appear when a user click on a link file with a powershell command in it
- category: data/rules/windows/process_creation
- level: medium
- id: 30e92f50-bb5a-4884-98b5-d20aa80f3d7a

Title: Suspicious Child Process Created as System
- description: Detection of child processes spawned with SYSTEM privileges by parents with LOCAL SERVICE or NETWORK SERVICE ac
- category: data/rules/windows/process_creation
- level: high
- id: 590a5f4c-6c8c-4f10-8307-89afe9453a9d

Title: Suspicious Parent of Csc.exe
- description: Detects a suspicious parent of csc.exe, which could by a sign of payload delivery
- category: data/rules/windows/process_creation
- level: high
- id: b730a276-6b63-41b8-bcf8-55930c8fc6ee

Title: Findstr GPP Passwords
- description: Look for the encrypted cpassword value within Group Policy Preference files on the Domain Controller. This valu
- category: data/rules/windows/process_creation
- level: high
- id: 91a2c315-9ee6-4052-a853-6f6a8238f90d

Title: Encoded FromBase64String
- description: Detects a base64 encoded FromBase64String keyword in a process command line
- category: data/rules/windows/process_creation
- level: critical
- id: fdb62a13-9a81-4e5c-a38f-ea93a16f6d7c

Title: Shells Spawned by Web Servers
- description: Web servers that spawn shell processes could be the result of a successfully placed web shell or an other attac
- category: data/rules/windows/process_creation
- level: high
- id: 8202070f-edeb-4d31-a010-a26c72ac5600

Title: BlueMashroom DLL Load
- description: Detects a suspicious DLL loading from AppData Local path as described in BlueMashroom report
- category: data/rules/windows/process_creation
- level: critical
- id: bd70d3f8-e60e-4d25-89f0-0b5a9cff20e0

Title: Rundll32 JS RunHTMLApplication Pattern
- description: Detects suspicious command line patterns used when rundll32 is used to run JavaScript code
- category: data/rules/windows/process_creation
- level: high
- id: 9f06447a-a33a-4cbe-a94f-a3f43184a7a3

Title: Renamed jusched.exe
- description: Detects renamed jusched.exe used by cobalt group
- category: data/rules/windows/process_creation
- level: high
- id: edd8a48c-1b9f-4ba1-83aa-490338cd1ccb

Title: MavInject Process Injection
- description: Detects process injection using the signed Windows tool Mavinject32.exe
- category: data/rules/windows/process_creation
- level: critical
- id: 17eb8e57-9983-420d-ad8a-2c4976c22eb8

Title: Dumpert Process Dumper
- description: Detects the use of Dumpert process dumper, which dumps the lsass.exe process memory
- category: data/rules/windows/process_creation
- level: critical
- id: 2704ab9e-afe2-4854-a3b1-0c0706d03578

Title: ScreenConnect Remote Access
- description: Detects ScreenConnect program starts that establish a remote access to that system (not meeting, not remote sup
- category: data/rules/windows/process_creation
- level: high
- id: 75bfe6e6-cd8e-429e-91d3-03921e1d7962

Title: Script Event Consumer Spawning Process
- description: Detects a suspicious child process of Script Event Consumer (scrcons.exe).
- category: data/rules/windows/process_creation
- level: high
- id: f6d1dd2f-b8ce-40ca-bc23-062efb686b34

Title: Use of GoToAssist Remote Access Software
- description: An adversary may use legitimate desktop support and remote access software, such as Team Viewer, Go2Assist, Log

These services are commonly used as legitimate technical support software, and may be allowed by application control within a target environment. Remote access tools like VNC, Ammyy, and Teamviewer are used frequently when compared with other legitimate software commonly used by adversaries. (Citation: Symantec Living off the Land)

- category: data/rules/windows/process_creation
- level: medium
- id: b6d98a4f-cef0-4abf-bbf6-24132854a83d

Title: CrackMapExec Command Execution
- description: Detect various execution methods of the CrackMapExec pentesting framework
- category: data/rules/windows/process_creation
- level: high
- id: 058f4380-962d-40a5-afce-50207d36d7e2

Title: Suspicious WMI Execution
- description: Detects WMI executing suspicious commands
- category: data/rules/windows/process_creation
- level: medium
- id: 526be59f-a573-4eea-b5f7-f0973207634d

Title: Squirrel Lolbin
- description: Detects Possible Squirrel Packages Manager as Lolbin
- category: data/rules/windows/process_creation
- level: medium
- id: fa4b21c9-0057-4493-b289-2556416ae4d7

Title: Obfuscated Command Line Using Special Unicode Characters
- description: Adversaries may attempt to make an executable or file difficult to discover or analyze by encrypting, encoding,
- category: data/rules/windows/process_creation
- level: high
- id: e0552b19-5a83-4222-b141-b36184bb8d79

Title: SOURGUM Actor Behaviours
- description: Suspicious behaviours related to an actor tracked by Microsoft as SOURGUM
- category: data/rules/windows/process_creation
- level: high

- id: 7ba08e95-1e0b-40cd-9db5-b980555e42fd

Title: Suspicious Scan Loop Network
- description: Adversaries may attempt to get a listing of other systems by IP address, hostname, or other logical identifier
- category: data/rules/windows/process_creation
- level: medium
- id: f8ad2e2c-40b6-4117-84d7-20b89896ab23

Title: Grabbing Sensitive Hives via Reg Utility
- description: Dump sam, system or security hives using REG.exe utility
- category: data/rules/windows/process_creation
- level: medium
- id: fd877b94-9bb5-4191-bb25-d79cbd93c167

Title: Control Panel Items
- description: Detects the malicious use of a control panel item
- category: data/rules/windows/process_creation
- level: critical
- id: 0ba863e6-def5-4e50-9cea-4dd8c7dc46a4

Title: Mavinject Inject DLL Into Running Process
- description: Injects arbitrary DLL into running process specified by process ID. Requires Windows 10.
- category: data/rules/windows/process_creation
- level: medium
- id: 4f73421b-5a0b-4bbf-a892-5a7fb99bea66

Title: DNS RCE CVE-2020-1350
- description: Detects exploitation of DNS RCE bug reported in CVE-2020-1350 by the detection of suspicious sub process
- category: data/rules/windows/process_creation
- level: critical
- id: b5281f31-f9cc-4d0d-95d0-45b91c45b487

Title: Winword LOLBIN Usage
- description: Winword can be abused as a LOLBIN to download arbitary file or load arbitary DLLs
- category: data/rules/windows/process_creation
- level: high
- id: 4ae3e30b-b03f-43aa-87e3-b622f4048eed

Title: Hiding Files with Attrib.exe
- description: Detects usage of attrib.exe to hide files from users.
- category: data/rules/windows/process_creation
- level: low
- id: 4281cb20-2994-4580-aa63-c8b86d019934

Title: DNS ServerLevelPluginDll Install
- description: Detects the installation of a plugin DLL via ServerLevelPluginDll parameter in Registry, which can be used to e
- category: data/rules/windows/process_creation
- level: high
- id: f63b56ee-3f79-4b8a-97fb-5c48007e8573

Title: Invoke-Obfuscation RUNDLL LAUNCHER
- description: Detects Obfuscated Powershell via RUNDLL LAUNCHER
- category: data/rules/windows/process_creation
- level: medium
- id: 056a7ee1-4853-4e67-86a0-3fd9ceed7555

Title: PowerShell SAM Copy
- description: Detects suspicious PowerShell scripts accessing SAM hives
- category: data/rules/windows/process_creation
- level: high
- id: 1af57a4b-460a-4738-9034-db68b880c665

Title: Suspicious Shells Spawn by Java
- description: Detects suspicious shell spawn from Java host process (e.g. log4j exploitation)
- category: data/rules/windows/process_creation
- level: high
- id: 0d34ed8b-1c12-4ff2-828c-16fc860b766d

Title: Suspicious Windows Update Agent Empty Cmdline

- description: Detects suspicious Windows Update Agent activity in which a wuauclt.exe process command line doesn't contain an
- category: data/rules/windows/process_creation
- level: high
- id: 52d097e2-063e-4c9c-8fbb-855c8948d135

Title: MSHTA Spwaned by SVCHOST
- description: Detects MSHTA.EXE spwaned by SVCHOST as seen in LethalHTA and described in report
- category: data/rules/windows/process_creation
- level: high
- id: ed5d72a6-f8f4-479d-ba79-02f6a80d7471

Title: Suspicious RDP Redirect Using TSCON
- description: Detects a suspicious RDP session redirect using tscon.exe
- category: data/rules/windows/process_creation
- level: high
- id: f72aa3e8-49f9-4c7d-bd74-f8ab84ff9bbb

Title: Proxy Execution via Wuauclt
- description: Detects the use of the Windows Update Client binary (wuauclt.exe) to proxy execute code.
- category: data/rules/windows/process_creation
- level: critical
- id: af77cf95-c469-471c-b6a0-946c685c4798

Title: Bypass UAC via Fodhelper.exe
- description: Identifies use of Fodhelper.exe to bypass User Account Control. Adversaries use this technique to execute privi
- category: data/rules/windows/process_creation
- level: high
- id: 7f741dcf-fc22-4759-87b4-9ae8376676a2

Title: TAIDOOR RAT DLL Load
- description: Detects specific process characteristics of Chinese TAIDOOR RAT malware load
- category: data/rules/windows/process_creation
- level: critical
- id: d1aa3382-abab-446f-96ea-4de52908210b

Title: Suspicious PowerShell Download and Execute Pattern
- description: Detects suspicious PowerShell download patterns that are often used in malicious scripts, stagers or downloader
- category: data/rules/windows/process_creation
- level: high
- id: e6c54d94-498c-4562-a37c-b469d8e9a275

Title: Suspicious Minimized MSEdge Start
- description: Detects the suspicious minimized start of MsEdge browser, which can be used to download files from the Internet
- category: data/rules/windows/process_creation
- level: high
- id: 94771a71-ba41-4b6e-a757-b531372eaab6

Title: Registry Disabling LSASS PPL
- description: Detects reg command lines that disables PPL on the LSA process
- category: data/rules/windows/process_creation
- level: high
- id: 8c0eca51-0f88-4db2-9183-fdfb10c703f9

Title: Microsoft Outlook Product Spawning Windows Shell
- description: Detects a Windows command and scripting interpreter executable started from Microsoft Outlook
- category: data/rules/windows/process_creation
- level: high
- id: 208748f7-881d-47ac-a29c-07ea84bf691d

Title: XORDump Use
- description: Detects suspicious use of XORDump process memory dumping utility
- category: data/rules/windows/process_creation
- level: high
- id: 66e563f9-1cbd-4a22-a957-d8b7c0f44372

Title: Suspicious Shells Spawn by WinRM
- description: Detects suspicious shell spawn from WinRM host process
- category: data/rules/windows/process_creation
- level: high

- id: 5cc2cda8-f261-4d88-a2de-e9e193c86716

Title: Suspicious Execution of Systeminfo
- description: Use of systeminfo to get information
- category: data/rules/windows/process_creation
- level: low
- id: 0ef56343-059e-4cb6-adc1-4c3c967c5e46

Title: Suspicious OfflineScannerShell.exe Execution From Another Folder
- description: Use OfflineScannerShell.exe to execute mpclient.dll library in the current working directory
- category: data/rules/windows/process_creation
- level: medium
- id: 02b18447-ea83-4b1b-8805-714a8a34546a

Title: Too Long PowerShell Commandlines
- description: Detects Too long PowerShell command lines
- category: data/rules/windows/process_creation
- level: medium
- id: d0d28567-4b9a-45e2-8bbc-fb1b66a1f7f6

Title: Abusing Windows Telemetry For Persistence
- description: Windows telemetry makes use of the binary CompatTelRunner.exe to run a variety of commands and perform the actu
- category: data/rules/windows/process_creation
- level: high
- id: f548a603-c9f2-4c89-b511-b089f7e94549

Title: Suspicious Redirection to Local Admin Share
- description: Detects a suspicious output redirection to the local admins share as often found in malicious scripts or hackto
- category: data/rules/windows/process_creation
- level: high
- id: ab9e3b40-0c85-4ba1-aede-455d226fd124

Title: New Service Creation
- description: Detects creation of a new service.
- category: data/rules/windows/process_creation
- level: low
- id: 7fe71fc9-de3b-432a-8d57-8c809efc10ab

Title: Suspicious ConfigSecurityPolicy Execution
- description: Upload file, credentials or data exfiltration with Binary part of Windows Defender
- category: data/rules/windows/process_creation
- level: medium
- id: 1f0f6176-6482-4027-b151-00071af39d7e

Title: Mounted Share Deleted
- description: Detects when when a mounted share is removed. Adversaries may remove share connections that are no longer usefu
- category: data/rules/windows/process_creation
- level: low
- id: cb7c4a03-2871-43c0-9bbb-18bbdb079896

Title: Use of PktMon.exe
- description: Tools to Capture Network Packets on the windows 10 with October 2018 Update or later.
- category: data/rules/windows/process_creation
- level: medium
- id: f956c7c1-0f60-4bc5-b7d7-b39ab3c08908

Title: Suspicious Debugger Registration Cmdline
- description: Detects the registration of a debugger for a program that is available in the logon screen (sticky key backdoor
- category: data/rules/windows/process_creation
- level: high
- id: ae215552-081e-44c7-805f-be16f975c8a2

Title: VMToolsd Suspicious Child Process
- description: Detects suspicious child process creations of VMware Tools process which may indicate persistence setup
- category: data/rules/windows/process_creation
- level: high
- id: 5687f942-867b-4578-ade7-1e341c46e99a

Title: SMB Relay Attack Tools

- description: Detects different hacktools used for relay attacks on Windows for privilege escalation
- category: data/rules/windows/process_creation
- level: critical
- id: 5589ab4f-a767-433c-961d-c91f3f704db1

Title: Execute Files with Msdeploy.exe
- description: Detects file execution using the msdeploy.exe lolbin
- category: data/rules/windows/process_creation
- level: medium
- id: 646bc99f-6682-4b47-a73a-17b1b64c9d34

Title: WMI Backdoor Exchange Transport Agent
- description: Detects a WMI backdoor in Exchange Transport Agents via WMI event filters
- category: data/rules/windows/process_creation
- level: critical
- id: 797011dc-44f4-4e6f-9f10-a8ceefbe566b

Title: Abusable Invoke-ATHRemoteFXvGPUDisablementCommand
- description: RemoteFXvGPUDisablement.exe is an abusable, signed PowerShell host executable that was introduced in Windows 10
- category: data/rules/windows/process_creation
- level: medium
- id: a6fc3c46-23b8-4996-9ea2-573f4c4d88c5

Title: Dumping Process via Sqldumper.exe
- description: Detects process dump via legitimate sqldumper.exe binary
- category: data/rules/windows/process_creation
- level: medium
- id: 23ceaf5c-b6f1-4a32-8559-f2ff734be516

Title: Powershell Reverse Shell Connection
- description: Detects the Nishang Invoke-PowerShellTcpOneLine reverse shell
- category: data/rules/windows/process_creation
- level: high
- id: edc2f8ae-2412-4dfd-b9d5-0c57727e70be

Title: PowerShell Web Download
- description: Detects suspicious ways to download files or content using PowerShell
- category: data/rules/windows/process_creation
- level: medium
- id: 6e897651-f157-4d8f-aaeb-df8151488385

Title: Default PowerSploit and Empire Schtasks Persistence
- description: Detects the creation of a schtask via PowerSploit or Empire Default Configuration.
- category: data/rules/windows/process_creation
- level: high
- id: 56c217c3-2de2-479b-990f-5c109ba8458f

Title: Reg Add RUN Key
- description: Detects suspicious command line reg.exe tool adding key to RUN key in Registry
- category: data/rules/windows/process_creation
- level: medium
- id: de587dce-915e-4218-aac4-835ca6af6f70

Title: Bypass UAC via WSReset.exe
- description: Identifies use of WSReset.exe to bypass User Account Control. Adversaries use this technique to execute privile
- category: data/rules/windows/process_creation
- level: high
- id: d797268e-28a9-49a7-b9a8-2f5039011c5c

Title: Suspicious Powershell No File or Command
- description: Detects suspicious powershell execution that ends with a common flag instead of a command or a filename to exec
- category: data/rules/windows/process_creation
- level: high
- id: b66474aa-bd92-4333-a16c-298155b120df

Title: Arbitrary Shell Command Execution Via Settingcontent-Ms
- description: The .SettingContent-ms file type was introduced in Windows 10 and allows a user to create "shortcuts" to variou
- category: data/rules/windows/process_creation
- level: medium

- id: 24de4f3b-804c-4165-b442-5a06a2302c7e

Title: Exploiting SetupComplete.cmd CVE-2019-1378
- description: Detects exploitation attempt of privilege escalation vulnerability via SetupComplete.cmd and PartnerSetupComple
- category: data/rules/windows/process_creation
- level: high
- id: 1c373b6d-76ce-4553-997d-8c1da9a6b5f5

Title: Disable or Delete Windows Eventlog
- description: Detects command that is used to disable or delete Windows eventlog via logman Windows utility
- category: data/rules/windows/process_creation
- level: high
- id: cd1f961e-0b96-436b-b7c6-38da4583ec00

Title: Suspicious File Characteristics Due to Missing Fields
- description: Detects Executables in the Downloads folder without FileVersion,Description,Product,Company likely created with
- category: data/rules/windows/process_creation
- level: medium
- id: 9637e8a5-7131-4f7f-bdc7-2b05d8670c43

Title: Usage of Sysinternals Tools
- description: Detects the usage of Sysinternals Tools due to accepteula key being added to Registry
- category: data/rules/windows/process_creation
- level: low
- id: 7cccd811-7ae9-4ebe-9afd-cb5c406b824b

Title: Cmd.exe CommandLine Path Traversal
- description: detects the usage of path traversal in cmd.exe indicating possible command/argument confusion/hijacking
- category: data/rules/windows/process_creation
- level: high
- id: 087790e3-3287-436c-bccf-cbd0184a7db1

Title: NotPetya Ransomware Activity
- description: Detects NotPetya ransomware activity in which the extracted passwords are passed back to the main module via na
- category: data/rules/windows/process_creation
- level: critical
- id: 79aeeb41-8156-4fac-a0cd-076495ab82a1

Title: Suspicious Certreq Command to Download
- description: Detects a suspicious certreq execution taken from the LOLBAS examples, which can be abused to download (small)
- category: data/rules/windows/process_creation
- level: high
- id: 4480827a-9799-4232-b2c4-ccc6c4e9e12b

Title: RunDLL32 Spawning Explorer
- description: Detects RunDLL32.exe spawning explorer.exe as child, which is very uncommon, often observes Gamarue spawning th
- category: data/rules/windows/process_creation
- level: high
- id: caa06de8-fdef-4c91-826a-7f9e163eef4b

Title: OpenWith.exe Executes Specified Binary
- description: The OpenWith.exe executes other binary
- category: data/rules/windows/process_creation
- level: high
- id: cec8e918-30f7-4e2d-9bfa-a59cc97ae60f

Title: Certutil Encode
- description: Detects suspicious a certutil command that used to encode files, which is sometimes used for data exfiltration
- category: data/rules/windows/process_creation
- level: medium
- id: e62a9f0c-ca1e-46b2-85d5-a6da77f86d1a

Title: Suspicious Dosfuscation Character in Commandline
- description: Posssible Payload Obfuscation
- category: data/rules/windows/process_creation
- level: medium
- id: a77c1610-fc73-4019-8e29-0f51efc04a51

Title: Trickbot Malware Activity

- description: Detects Trickbot malware process tree pattern in which rundll32.exe is parent of wermgr.exe
- category: data/rules/windows/process_creation
- level: critical
- id: 58bf96d9-ff5f-44bd-8dcc-1c4f79bf3a27

Title: JSC Convert Javascript To Executable
- description: Detects the execution of the LOLBIN jsc.exe used by .NET to compile javascript code to .exe or .dll format
- category: data/rules/windows/process_creation
- level: medium
- id: 52788a70-f1da-40dd-8fbd-73b5865d6568

Title: Recon Activity with NLTEST
- description: Detects nltest commands that can be used for information discovery
- category: data/rules/windows/process_creation
- level: medium
- id: 5cc90652-4cbd-4241-aa3b-4b462fa5a248

Title: Suspicious PowerShell Invocation Based on Parent Process
- description: Detects suspicious powershell invocations from interpreters or unusual programs
- category: data/rules/windows/process_creation
- level: medium
- id: 95eadcb2-92e4-4ed1-9031-92547773a6db

Title: Chafer Activity
- description: Detects Chafer activity attributed to OilRig as reported in Nyotron report in March 2018
- category: data/rules/windows/process_creation
- level: critical
- id: ce6e34ca-966d-41c9-8d93-5b06c8b97a06

Title: Bitsadmin Download
- description: Detects usage of bitsadmin downloading a file
- category: data/rules/windows/process_creation
- level: medium
- id: d059842b-6b9d-4ed1-b5c3-5b89143c6ede

Title: GALLIUM Artefacts
- description: Detects artefacts associated with activity group GALLIUM - Microsoft Threat Intelligence Center indicators rele
- category: data/rules/windows/process_creation
- level: high
- id: 18739897-21b1-41da-8ee4-5b786915a676

Title: LOLBAS Data Exfiltration by DataSvcUtil.exe
- description: Detects when a user performs data exfiltration by using DataSvcUtil.exe
- category: data/rules/windows/process_creation
- level: medium
- id: e290b10b-1023-4452-a4a9-eb31a9013b3a

Title: Invoke-Obfuscation Via Use MSHTA
- description: Detects Obfuscated Powershell via use MSHTA in Scripts
- category: data/rules/windows/process_creation
- level: high
- id: ac20ae82-8758-4f38-958e-b44a3140ca88

Title: Suspicious Del in CommandLine
- description: suspicious command line to remove exe or dll
- category: data/rules/windows/process_creation
- level: medium
- id: 204b17ae-4007-471b-917b-b917b315c5db

Title: Regedit as Trusted Installer
- description: Detects a regedit started with TrustedInstaller privileges or by ProcessHacker.exe
- category: data/rules/windows/process_creation
- level: high
- id: 883835a7-df45-43e4-bf1d-4268768afda4

Title: Powershell Defender Disable Scan Feature
- description: Detects requests to disable Microsoft Defender features using PowerShell commands
- category: data/rules/windows/process_creation
- level: high

- id: 1ec65a5f-9473-4f12-97da-622044d6df21

Title: Suspicious Query of MachineGUID
- description: Use of reg to get MachineGuid information
- category: data/rules/windows/process_creation
- level: low
- id: f5240972-3938-4e56-8e4b-e33893176c1f

Title: Always Install Elevated Windows Installer
- description: This rule looks for Windows Installer service (msiexec.exe) trying to install MSI packages with SYSTEM privileg
- category: data/rules/windows/process_creation
- level: medium
- id: cd951fdc-4b2f-47f5-ba99-a33bf61e3770

Title: Run Whoami as SYSTEM
- description: Detects a whoami.exe executed by LOCAL SYSTEM. This may be a sign of a successful local privilege escalation.
- category: data/rules/windows/process_creation
- level: high
- id: 80167ada-7a12-41ed-b8e9-aa47195c66a1

Title: Lolbins Process Creation with WmiPrvse
- description: This rule will monitor LOLBin process creations by wmiprvse. Add more LOLBins to rule logic if needed.
- category: data/rules/windows/process_creation
- level: high
- id: 8a582fe2-0882-4b89-a82a-da6b2dc32937

Title: Suspicious Ntdll Pipe Redirection
- description: Detects command that type the content of ntdll.dll to a different file or a pipe in order to evade AV / EDR det
- category: data/rules/windows/process_creation
- level: high
- id: bbc865e4-7fcd-45a6-8ff1-95ced28ec5b2

Title: Dotnet.exe Exec Dll and Execute Unsigned Code LOLBIN
- description: dotnet.exe will execute any DLL and execute unsigned code
- category: data/rules/windows/process_creation
- level: medium
- id: d80d5c81-04ba-45b4-84e4-92eba40e0ad3

Title: Windows Processes Suspicious Parent Directory
- description: Detect suspicious parent processes of well-known Windows processes
- category: data/rules/windows/process_creation
- level: low
- id: 96036718-71cc-4027-a538-d1587e0006a7

Title: Netsh Port or Application Allowed
- description: Allow Incoming Connections by Port or Application on Windows Firewall
- category: data/rules/windows/process_creation
- level: medium
- id: cd5cfd80-aa5f-44c0-9c20-108c4ae12e3c

Title: Suspicious Code Page Switch
- description: Detects a code page switch in command line or batch scripts to a rare language
- category: data/rules/windows/process_creation
- level: medium
- id: c7942406-33dd-4377-a564-0f62db0593a3

Title: Suspicious VBScript UN2452 Pattern
- description: Detects suspicious inline VBScript keywords as used by UNC2452
- category: data/rules/windows/process_creation
- level: high
- id: 20c3f09d-c53d-4e85-8b74-6aa50e2f1b61

Title: Write Protect For Storage Disabled
- description: Looks for changes to registry to disable any write-protect property for storage devices. This could be a precur
- category: data/rules/windows/process_creation
- level: medium
- id: 75f7a0e2-7154-4c4d-9eae-5cdb4e0a5c13

Title: Suspicious Registration via cscript.exe

- description: Detects when the registration of a VSS/VDS Provider as a COM+ application.
- category: data/rules/windows/process_creation
- level: medium
- id: 28c8f68b-098d-45af-8d43-8089f3e35403

Title: Time Travel Debugging Utility Usage
- description: Detects usage of Time Travel Debugging Utility. Adversaries can execute malicious processes and dump processes,
- category: data/rules/windows/process_creation
- level: high
- id: 0b4ae027-2a2d-4b93-8c7e-962caaba5b2a

Title: Judgement Panda Exfil Activity
- description: Detects Judgement Panda activity as described in Global Threat Report 2019 by Crowdstrike
- category: data/rules/windows/process_creation
- level: critical
- id: 03e2746e-2b31-42f1-ab7a-eb39365b2422

Title: BlackByte Ransomware Patterns
- description: This command line patterns found in BlackByte Ransomware operations
- category: data/rules/windows/process_creation
- level: high
- id: 999e8307-a775-4d5f-addc-4855632335be

Title: Abuse of Service Permissions to Hide Services in Tools
- description: Detection of sc.exe utility adding a new service with special permission which hides that service.
- category: data/rules/windows/process_creation
- level: high
- id: a537cfc3-4297-4789-92b5-345bfd845ad0

Title: MSHTA Suspicious Execution 01
- description: Detection for mshta.exe suspicious execution patterns sometimes involving file polyglotism
- category: data/rules/windows/process_creation
- level: high
- id: cc7abbd0-762b-41e3-8a26-57ad50d2eea3

Title: Suspicious PrinterPorts Creation (CVE-2020-1048)
- description: Detects new commands that add new printer port which point to suspicious file
- category: data/rules/windows/process_creation
- level: high
- id: cc08d590-8b90-413a-aff6-31d1a99678d7

Title: Suspicious Execution from Outlook
- description: Detects EnableUnsafeClientMailRules used for Script Execution from Outlook
- category: data/rules/windows/process_creation
- level: high
- id: e212d415-0e93-435f-9e1a-f29005bb4723

Title: AWL Bypass with Winrm.vbs and Malicious WsmPty.xsl/WsmTxt.xsl
- description: Detects execution of attacker-controlled WsmPty.xsl or WsmTxt.xsl via winrm.vbs and copied cscript.exe (can be
- category: data/rules/windows/process_creation
- level: medium
- id: 074e0ded-6ced-4ebd-8b4d-53f55908119d

Title: Suspicious Add Scheduled Command Pattern
- description: Detects suspicious scheduled task creations with commands that are uncommon
- category: data/rules/windows/process_creation
- level: high
- id: f2c64357-b1d2-41b7-849f-34d2682c0fad

Title: Windows Cmd Delete File
- description: Adversaries may delete files left behind by the actions of their intrusion activity.

Malware, tools, or other non-native files dropped or created on a system by an adversary may leave traces to indicate to what was done within a network and how. Removal of these files can occur during an intrusion, or as part of a post-intrusion process to minimize the adversary's footprint.

- category: data/rules/windows/process_creation
- level: low
- id: 379fa130-190e-4c3f-b7bc-6c8e834485f3

Title: Taskmgr as Parent
- description: Detects the creation of a process from Windows task manager
- category: data/rules/windows/process_creation
- level: low
- id: 3d7679bd-0c00-440c-97b0-3f204273e6c7

Title: Exploiting CVE-2019-1388
- description: Detects an exploitation attempt in which the UAC consent dialogue is used to invoke an Internet Explorer proces
- category: data/rules/windows/process_creation
- level: critical
- id: 02e0b2ea-a597-428e-b04a-af6a1a403e5c

Title: Suspicious MsiExec Directory
- description: Detects suspicious msiexec process starts in an uncommon directory
- category: data/rules/windows/process_creation
- level: high
- id: e22a6eb2-f8a5-44b5-8b44-a2dbd47b1144

Title: Suspicious Get Local Groups Information with WMIC
- description: Adversaries may attempt to find local system groups and permission settings.

The knowledge of local system permission groups can help adversaries determine which groups exist and which users belong to a particular group. Adversaries may use this information to determine which users have elevated permissions, such as the users found within the local administrators group.

- category: data/rules/windows/process_creation
- level: low
- id: 164eda96-11b2-430b-85ff-6a265c15bf32

Title: Impacket Lateralization Detection
- description: Detects wmiexec/dcomexec/atexec/smbexec from Impacket framework
- category: data/rules/windows/process_creation
- level: critical
- id: 10c14723-61c7-4c75-92ca-9af245723ad2

Title: Esentutl Steals Browser Information
- description: One way Qbot steals sensitive information is by extracting browser data from Internet Explorer and Microsoft Ed
- category: data/rules/windows/process_creation
- level: medium
- id: 6a69f62d-ce75-4b57-8dce-6351eb55b362

Title: Execution in Outlook Temp Folder
- description: Detects a suspicious program execution in Outlook temp folder
- category: data/rules/windows/process_creation
- level: high
- id: a018fdc3-46a3-44e5-9afb-2cd4af1d4b39

Title: Credential Dumping Tools Service Execution
- description: Detects well-known credential dumping tools execution via service execution events
- category: data/rules/windows/driver_load
- level: critical
- id: df5ff0a5-f83f-4a5b-bba1-3e6a3f6f6ea2

Title: WinDivert Driver Load
- description: Detects the load of the Windiver driver, a powerful user-mode capture/sniffing/modification/blocking/re-injecti
- category: data/rules/windows/driver_load
- level: high
- id: 679085d5-f427-4484-9f58-1dc30a7c426d

Title: Meterpreter or Cobalt Strike Getsystem Service Installation
- description: Detects the use of getsystem Meterpreter/Cobalt Strike command by detecting a specific service installation
- category: data/rules/windows/driver_load
- level: critical
- id: d585ab5a-6a69-49a8-96e8-4a726a54de46

Title: Vulnerable Dell BIOS Update Driver Load
- description: Detects the load of the vulnerable Dell BIOS update driver as reported in CVE-2021-21551
- category: data/rules/windows/driver_load
- level: high
- id: 21b23707-60d6-41bb-96e3-0f0481b0fed9

Title: Suspicious Driver Load from Temp
- description: Detects a driver load from a temporary directory
- category: data/rules/windows/driver_load
- level: high
- id: 2c4523d5-d481-4ed0-8ec3-7fbf0cb41a75

Title: PowerShell Scripts Run by a Services
- description: Detects powershell script installed as a Service
- category: data/rules/windows/driver_load
- level: high
- id: 46deb5e1-28c9-4905-b2df-51cdcc9e6073

Title: Suspicious desktop.ini Action
- description: Detects unusual processes accessing desktop.ini, which can be leveraged to alter how Explorer displays a folder
- category: data/rules/windows/file_event
- level: medium
- id: 81315b50-6b60-4d8f-9928-3466e1022515

Title: CVE-2021-1675 Print Spooler Exploitation Filename Pattern
- description: Detects the default filename used in PoC code against print spooler vulnerability CVE-2021-1675
- category: data/rules/windows/file_event
- level: critical
- id: 2131cfb3-8c12-45e8-8fa0-31f5924e9f07

Title: Hijack Legit RDP Session to Move Laterally
- description: Detects the usage of tsclient share to place a backdoor on the RDP source machine's startup folder
- category: data/rules/windows/file_event
- level: high
- id: 52753ea4-b3a0-4365-910d-36cff487b789

Title: UAC Bypass Using NTFS Reparse Point - File
- description: Detects the pattern of UAC Bypass using NTFS reparse point and wusa.exe DLL hijacking (UACMe 36)
- category: data/rules/windows/file_event
- level: high
- id: 7fff6773-2baa-46de-a24a-b6eec1aba2d1

Title: WMI Persistence - Script Event Consumer File Write
- description: Detects file writes of WMI script event consumer
- category: data/rules/windows/file_event
- level: high
- id: 33f41cdd-35ac-4ba8-814b-c6a4244a1ad4

Title: Advanced IP Scanner
- description: Detects the use of Advanced IP Scanner. Seems to be a popular tool for ransomware groups.
- category: data/rules/windows/file_event
- level: medium
- id: fed85bf9-e075-4280-9159-fbe8a023d6fa

Title: LSASS Process Memory Dump Files
- description: Detects file names used by different memory dumping tools to create a memory dump of the LSASS process memory,
- category: data/rules/windows/file_event
- level: high
- id: a5a2d357-1ab8-4675-a967-ef9990a59391

Title: LSASS Memory Dump File Creation
- description: LSASS memory dump creation using operating systems utilities. Procdump will use process name in output file if
- category: data/rules/windows/file_event
- level: high
- id: 5e3d3601-0662-4af0-b1d2-36a05e90c40a

Title: NPPSpy Hacktool Usage
- description: Detects the use of NPPSpy hacktool that stores cleartext passwords of users that logged in to a local file
- category: data/rules/windows/file_event
- level: high
- id: cad1fe90-2406-44dc-bd03-59d0b58fe722

Title: Suspicious Files in Default GPO Folder
- description: Detects the creation of copy of suspicious files (EXE/DLL) to the default GPO storage folder

- category: data/rules/windows/file_event
- level: medium
- id: 5f87308a-0a5b-4623-ae15-d8fa1809bc60

Title: PowerShell Writing Startup Shortcuts
- description: Attempts to detect PowerShell writing startup shortcuts. This procedure was highlighted in Red Canary Intel Ins
- category: data/rules/windows/file_event
- level: high
- id: 92fa78e7-4d39-45f1-91a3-8b23f3f1088d

Title: Suspicious MSExchangeMailboxReplication ASPX Write
- description: Detects suspicious activity in which the MSExchangeMailboxReplication process writes .asp and .apsx files to di
- category: data/rules/windows/file_event
- level: high
- id: 7280c9f3-a5af-45d0-916a-bc01cb4151c9

Title: GoToAssist Temporary Installation Artefact
- description: An adversary may use legitimate desktop support and remote access software, such as Team Viewer, Go2Assist, Log

These services are commonly used as legitimate technical support software, and may be allowed by application control within a target environment. Remote access tools like VNC, Ammyy, and Teamviewer are used frequently when compared with other legitimate software commonly used by adversaries. (Citation: Symantec Living off the Land)

- category: data/rules/windows/file_event
- level: medium
- id: 5d756aee-ad3e-4306-ad95-cb1abec48de2

Title: Suspicious Creation TXT File in User Desktop
- description: Ransomware create txt file in the user Desktop
- category: data/rules/windows/file_event
- level: high
- id: caf02a0a-1e1c-4552-9b48-5e070bd88d11

Title: Dynamic C Sharp Compile Artefact
- description: When C# is compiled dynamically, a .cmdline file will be created as a part of the process.

Certain processes are not typically observed compiling C# code, but can do so without touching disk. This can be used to unpack a payload for execution

- category: data/rules/windows/file_event
- level: low
- id: e4a74e34-ecde-4aab-b2fb-9112dd01aed0

Title: UAC Bypass Using EventVwr
- description: Detects the pattern of a UAC bypass using Windows Event Viewer
- category: data/rules/windows/file_event
- level: high
- id: 63e4f530-65dc-49cc-8f80-ccfa95c69d43

Title: Suspicious Word Cab File Write CVE-2021-40444
- description: Detects file creation patterns noticeable during the exploitation of CVE-2021-40444
- category: data/rules/windows/file_event
- level: critical
- id: 60c0a111-787a-4e8a-9262-ee485f3ef9d5

Title: New Shim Database Created in the Default Directory
- description: Adversaries may establish persistence and/or elevate privileges by executing malicious content triggered by app

The Microsoft Windows Application Compatibility Infrastructure/Framework (Application Shim) was created to allow for backward compatibility of software as the operating system codebase changes over time.

- category: data/rules/windows/file_event
- level: medium
- id: ee63c85c-6d51-4d12-ad09-04e25877a947

Title: PsExec Tool Execution
- description: Detects PsExec service installation and execution events (service and Sysmon)
- category: data/rules/windows/file_event
- level: low
- id: 259e5a6a-b8d2-4c38-86e2-26c5e651361d

Title: Suspicious Get-Variable.exe Creation
- description: Get-Variable is a valid PowerShell cmdlet

WindowsApps is by default in the path where PowerShell is executed. So when the Get-Variable command is issued on PowerShell execution, the system first looks for the Get-Variable executable in the path and executes the malicious binary instead of looking for the PowerShell cmdlet.

- category: data/rules/windows/file_event
- level: high
- id: 0c3fac91-5627-46e8-a6a8-a0d7b9b8ae1b

Title: Suspicious NTDS.DIT Creation
- description: Detects suspicious creations of a file named ntds.dit, e.g. by a PowerShell parent or in a suspicious directory
- category: data/rules/windows/file_event
- level: high
- id: 4e7050dd-e548-483f-b7d6-527ab4fa784d

Title: Powerup Write Hijack DLL
- description: Powerup tool's Write Hijack DLL exploits DLL hijacking for privilege escalation. In it's default mode, it build
- category: data/rules/windows/file_event
- level: high
- id: 602a1f13-c640-4d73-b053-be9a2fa58b96

Title: Suspicious Scheduled Task Write to System32 Tasks
- description: Detects the creation of tasks from processes executed from suspicious locations
- category: data/rules/windows/file_event
- level: high
- id: 80e1f67a-4596-4351-98f5-a9c3efabac95

Title: Malicious PowerShell Commandlet Names
- description: Detects the creation of known powershell scripts for exploitation
- category: data/rules/windows/file_event
- level: high
- id: f331aa1f-8c53-4fc3-b083-cc159bc971cb

Title: PCRE.NET Package Temp Files
- description: Detects processes creating temp files related to PCRE.NET package
- category: data/rules/windows/file_event
- level: high
- id: 6e90ae7a-7cd3-473f-a035-4ebb72d961da

Title: Startup Folder File Write
- description: A General detection for files being created in the Windows startup directory. This could be an indicator of per
- category: data/rules/windows/file_event
- level: low
- id: 2aa0a6b4-a865-495b-ab51-c28249537b75

Title: RedMimicry Winnti Playbook Dropped File
- description: Detects actions caused by the RedMimicry Winnti playbook
- category: data/rules/windows/file_event
- level: high
- id: 130c9e58-28ac-4f83-8574-0a4cc913b97e

Title: Suspicious Screensaver Binary File Creation
- description: Adversaries may establish persistence by executing malicious content triggered by user inactivity.

Screensavers are programs that execute after a configurable time of user inactivity and consist of Portable Executable (PE) files with a .scr file extension

- category: data/rules/windows/file_event
- level: medium
- id: 97aa2e88-555c-450d-85a6-229bcd87efb8

Title: Creation of an WerFault.exe in Unusual Folder
- description: Detects WerFault copoed to a suspicious folder, which could be a sign of WerFault DLL hijacking
- category: data/rules/windows/file_event
- level: high
- id: 28a452f3-786c-4fd8-b8f2-bddbe9d616d1

Title: Rclone Config File Creation
- description: Detects Rclone config file being created
- category: data/rules/windows/file_event

- level: high
- id: 34986307-b7f4-49be-92f3-e7a4d01ac5db

Title: SCR File Write Event
- description: An attacker may execute an application as a .SCR File (Screensaver) using rundll32.exe desk.cpl,InstallScreenSa
- category: data/rules/windows/file_event
- level: medium
- id: c048f047-7e2a-4888-b302-55f509d4a91d

Title: Outlook Form Installation
- description: Detects the creation of new Outlook form which can contain malicious code
- category: data/rules/windows/file_event
- level: high
- id: c3edc6a5-d9d4-48d8-930e-aab518390917

Title: Dumpert Process Dumper
- description: Detects the use of Dumpert process dumper, which dumps the lsass.exe process memory
- category: data/rules/windows/file_event
- level: critical
- id: 93d94efc-d7ad-4161-ad7d-1638c4f908d8

Title: CVE-2021-31979 CVE-2021-33771 Exploits by Sourgum
- description: Detects patterns as noticed in exploitation of Windows CVE-2021-31979 CVE-2021-33771 vulnerability and DevilsTo
- category: data/rules/windows/file_event
- level: critical
- id: ad7085ac-92e4-4b76-8ce2-276d2c0e68ef

Title: Created Files by Office Applications
- description: This rule will monitor executable and script file creation by office applications. Please add more file extensi
- category: data/rules/windows/file_event
- level: high
- id: c7a74c80-ba5a-486e-9974-ab9e682bc5e4

Title: CVE-2022-24527 Microsoft Connected Cache LPE
- description: Detects files created during the local privilege exploitation of CVE-2022-24527 Microsoft Connected Cache
- category: data/rules/windows/file_event
- level: high
- id: e0a41412-c69a-446f-8e6e-0e6d7483dad7

Title: Cred Dump Tools Dropped Files
- description: Files with well-known filenames (parts of credential dump software or files produced by them) creation
- category: data/rules/windows/file_event
- level: high
- id: 8fbf3271-1ef6-4e94-8210-03c2317947f6

Title: Anydesk Temporary Artefact
- description: An adversary may use legitimate desktop support and remote access software, such as Team Viewer, Go2Assist, Log

These services are commonly used as legitimate technical support software, and may be allowed by application control within a target environment. Remote access tools like VNC, Ammyy, and Teamviewer are used frequently when compared with other legitimate software commonly used by adversaries. (Citation: Symantec Living off the Land)

- category: data/rules/windows/file_event
- level: medium
- id: 0b9ad457-2554-44c1-82c2-d56a99c42377

Title: AWL Bypass with Winrm.vbs and Malicious WsmPty.xsl/WsmTxt.xsl
- description: Detects execution of attacker-controlled WsmPty.xsl or WsmTxt.xsl via winrm.vbs and copied cscript.exe (can be
- category: data/rules/windows/file_event
- level: medium
- id: d353dac0-1b41-46c2-820c-d7d2561fc6ed

Title: Creation Exe for Service with Unquoted Path
- description: Adversaries may execute their own malicious payloads by hijacking vulnerable file path references.

Adversaries can take advantage of paths that lack surrounding quotations by placing an executable in a higher level directory within the path, so that Windows will choose the adversary's executable to launch.

- category: data/rules/windows/file_event
- level: high

- id: 8c3c76ca-8f8b-4b1d-aaf3-81aebcd367c9

Title: Suspcious CLR Logs Creation
- description: Detects suspicious .NET assembly executions. Could detect using Cobalt Strike's command execute-assembly.
- category: data/rules/windows/file_event
- level: high
- id: e4b63079-6198-405c-abd7-3fe8b0ce3263

Title: UAC Bypass Using MSConfig Token Modification - File
- description: Detects the pattern of UAC Bypass using a msconfig GUI hack (UACMe 55)
- category: data/rules/windows/file_event
- level: high
- id: 41bb431f-56d8-4691-bb56-ed34e390906f

Title: WScript or CScript Dropper
- description: Detects a file ending in jse, vbe, js, vba, vbs written by cscript.exe or wscript.exe
- category: data/rules/windows/file_event
- level: high
- id: 002bdb95-0cf1-46a6-9e08-d38c128a6127

Title: Installation of TeamViewer Desktop
- description: TeamViewer_Desktop.exe is create during install
- category: data/rules/windows/file_event
- level: medium
- id: 9711de76-5d4f-4c50-a94f-21e4e8f8384d

Title: Suspicious NTDS Exfil Filename Patterns
- description: Detects suspicious creations of files with names used in various tools that export the NTDS.DIT for exfiltratio
- category: data/rules/windows/file_event
- level: high
- id: 3a8da4e0-36c1-40d2-8b29-b3e890d5172a

Title: SAM Dump File Creation
- description: Detects the creation of files that look like exports of the local SAM (Security Account Manager)
- category: data/rules/windows/file_event
- level: high
- id: 4e87b8e2-2ee9-4b2a-a715-4727d297ece0

Title: Powershell Profile.ps1 Modification
- description: Detects a change in profile.ps1 of the Powershell profile
- category: data/rules/windows/file_event
- level: high
- id: b5b78988-486d-4a80-b991-930eff3ff8bf

Title: ISO or Image Mount Indicator in Recent Files
- description: Detects the creation of recent element file that points to an .ISO, .IMG, .VHD or .VHDX file as often used in p
- category: data/rules/windows/file_event
- level: medium
- id: 4358e5a5-7542-4dcb-b9f3-87667371839b

Title: Mimikatz MemSSP Default Log File Creation
- description: Detects Mimikatz MemSSP default log file creation
- category: data/rules/windows/file_event
- level: critical
- id: 034affe8-6170-11ec-844f-0f78aa0c4d66

Title: Windows Shell File Write to Suspicious Folder
- description: Detects a Windows executable that writes files to suspicious folders
- category: data/rules/windows/file_event
- level: high
- id: 1277f594-a7d1-4f28-a2d3-73af5cbeab43

Title: CrackMapExec File Creation Patterns
- description: Detects suspicious file creation patterns found in logs when CrackMapExec is used
- category: data/rules/windows/file_event
- level: high
- id: 9433ff9c-5d3f-4269-99f8-95fc826ea489

Title: Outlook C2 Macro Creation

- description: Detects the creation of a macro file for Outlook. Goes with win_outlook_c2_registry_key. VbaProject.OTM is expl
- category: data/rules/windows/file_event
- level: medium
- id: 8c31f563-f9a7-450c-bfa8-35f8f32f1f61

Title: Windows Webshell Creation
- description: Possible webshell file creation on a static web site
- category: data/rules/windows/file_event
- level: critical
- id: 39f1f9f2-9636-45de-98f6-a4046aa8e4b9

Title: Detection of SafetyKatz
- description: Detects possible SafetyKatz Behaviour
- category: data/rules/windows/file_event
- level: high
- id: e074832a-eada-4fd7-94a1-10642b130e16

Title: Typical HiveNightmare SAM File Export
- description: Detects files written by the different tools that exploit HiveNightmare
- category: data/rules/windows/file_event
- level: high
- id: 6ea858a8-ba71-4a12-b2cc-5d83312404c7

Title: Suspicious Unattend.xml File Access
- description: Attempts to access unattend.xml, where credentials are commonly stored, within the Panther directory where inst

If these files exist, their contents will be displayed. They are used to store credentials/answers during the unattended windows install process

- category: data/rules/windows/file_event
- level: medium
- id: 1a3d42dd-3763-46b9-8025-b5f17f340dfb

Title: Unidentified Attacker November 2018
- description: A sigma rule detecting an unidetefied attacker who used phishing emails to target high profile orgs on November
- category: data/rules/windows/file_event
- level: high
- id: 3a3f81ca-652c-482b-adeb-b1c804727f74

Title: Suspicious PROCEXP152.sys File Created In TMP
- description: Detects the creation of the PROCEXP152.sys file in the application-data local temporary folder. This driver is
- category: data/rules/windows/file_event
- level: medium
- id: 3da70954-0f2c-4103-adff-b7440368f50e

Title: UAC Bypass Using Consent and Comctl32 - File
- description: Detects the pattern of UAC Bypass using consent.exe and comctl32.dll (UACMe 22)
- category: data/rules/windows/file_event
- level: high
- id: 62ed5b55-f991-406a-85d9-e8e8fdf18789

Title: TeamViewer Remote Session
- description: Detects the creation of log files during a TeamViewer remote session
- category: data/rules/windows/file_event
- level: medium
- id: 162ab1e4-6874-4564-853c-53ec3ab8be01

Title: Suspicious Interactive PowerShell as SYSTEM
- description: Detects the creation of files that indicator an interactive use of PowerShell in the SYSTEM user context
- category: data/rules/windows/file_event
- level: high
- id: 5b40a734-99b6-4b98-a1d0-1cea51a08ab2

Title: CVE-2021-26858 Exchange Exploitation
- description: Detects possible successful exploitation for vulnerability described in CVE-2021-26858 by looking for | creatio
- category: data/rules/windows/file_event
- level: critical
- id: b06335b3-55ac-4b41-937e-16b7f5d57dfd

Title: Wmiprvse Wbemcomn DLL Hijack

- description: Detects a threat actor creating a file named `wbemcomn.dll` in the `C:\Windows\System32\wbem\` directory over t
- category: data/rules/windows/file_event
- level: critical
- id: 614a7e17-5643-4d89-b6fe-f9df1a79641c

Title: Mimikatz Kirbi File Creation
- description: Detects the creation of files that contain Kerberos tickets based on an extension used by the popular tool Mimi
- category: data/rules/windows/file_event
- level: critical
- id: 9e099d99-44c2-42b6-a6d8-54c3545cab29

Title: Dump Office Macro Files from Commandline
- description: A office file with macro is created from a commandline or a script
- category: data/rules/windows/file_event
- level: medium
- id: b1c50487-1967-4315-a026-6491686d860e

Title: Octopus Scanner Malware
- description: Detects Octopus Scanner Malware.
- category: data/rules/windows/file_event
- level: high
- id: 805c55d9-31e6-4846-9878-c34c75054fe9

Title: Writing Local Admin Share
- description: Aversaries may use to interact with a remote network share using Server Message Block (SMB).

This technique is used by post-exploitation frameworks.

- category: data/rules/windows/file_event
- level: medium
- id: 4aafb0fa-bff5-4b9d-b99e-8093e659c65f

Title: Pingback Backdoor
- description: Detects the use of Pingback backdoor that creates ICMP tunnel for C2 as described in the trustwave report
- category: data/rules/windows/file_event
- level: high
- id: 2bd63d53-84d4-4210-80ff-bf0658f1bf78

Title: Suspicious PFX File Creation
- description: A general detection for processes creating PFX files. This could be an indicator of an adversary exporting a lo
- category: data/rules/windows/file_event
- level: medium
- id: dca1b3e8-e043-4ec8-85d7-867f334b5724

Title: Suspicious VHD Image Download From Browser
- description: Malware can use mountable Virtual Hard Disk .vhd file to encapsulate payloads and evade security controls
- category: data/rules/windows/file_event
- level: medium
- id: 8468111a-ef07-4654-903b-b863a80bbc95

Title: Suspicious ADSI-Cache Usage By Unknown Tool
- description: Detects the usage of ADSI (LDAP) operations by tools. This may also detect tools like LDAPFragger.
- category: data/rules/windows/file_event
- level: high
- id: 75bf09fa-1dd7-4d18-9af9-dd9e492562eb

Title: Microsoft Office Add-In Loading
- description: Detects add-ins that load when Microsoft Word or Excel starts (.wll/.xll are simply .dll fit for Word or Excel)
- category: data/rules/windows/file_event
- level: high
- id: 8e1cb247-6cf6-42fa-b440-3f27d57e9936

Title: UAC Bypass Abusing Winsat Path Parsing - File
- description: Detects the pattern of UAC Bypass using a path parsing issue in winsat.exe (UACMe 52)
- category: data/rules/windows/file_event
- level: high
- id: 155dbf56-e0a4-4dd0-8905-8a98705045e8

Title: UAC Bypass Using Windows Media Player - File

- description: Detects the pattern of UAC Bypass using Windows Media Player osksupport.dll (UACMe 32)
- category: data/rules/windows/file_event
- level: high
- id: 68578b43-65df-4f81-9a9b-92f32711a951

Title: Suspicious Desktopimgdownldr Target File
- description: Detects a suspicious Microsoft desktopimgdownldr file creation that stores a file to a suspicious location or c
- category: data/rules/windows/file_event
- level: high
- id: fc4f4817-0c53-4683-a4ee-b17a64bc1039

Title: Created Files by Microsoft Sync Center
- description: This rule detects suspicious files created by Microsoft Sync Center (mobsync)
- category: data/rules/windows/file_event
- level: medium
- id: 409f8a98-4496-4aaa-818a-c931c0a8b832

Title: ScreenConnect Temporary Installation Artefact
- description: An adversary may use legitimate desktop support and remote access software, such as Team Viewer, Go2Assist, Log

These services are commonly used as legitimate technical support software, and may be allowed by application control within a target environment. Remote access tools like VNC, Ammyy, and Teamviewer are used frequently when compared with other legitimate software commonly used by adversaries. (Citation: Symantec Living off the Land)

- category: data/rules/windows/file_event
- level: medium
- id: fec96f39-988b-4586-b746-b93d59fd1922

Title: File Created with System Process Name
- description: Detects the creation of an executable with a system process name in a suspicious folder
- category: data/rules/windows/file_event
- level: high
- id: d5866ddf-ce8f-4aea-b28e-d96485a20d3d

Title: UAC Bypass Using .NET Code Profiler on MMC
- description: Detects the pattern of UAC Bypass using .NET Code Profiler and mmc.exe DLL hijacking (UACMe 39)
- category: data/rules/windows/file_event
- level: high
- id: 93a19907-d4f9-4deb-9f91-aac4692776a6

Title: Moriya Rootkit
- description: Detects the use of Moriya rootkit as described in the securelist's Operation TunnelSnake report
- category: data/rules/windows/file_event
- level: critical
- id: a1507d71-0b60-44f6-b17c-bf53220fdd88

Title: InstallerFileTakeOver LPE CVE-2021-41379 File Create Event
- description: Detects signs of the exploitation of LPE CVE-2021-41379 that include an msiexec process that creates an elevati
- category: data/rules/windows/file_event
- level: critical
- id: 3be82d5d-09fe-4d6a-a275-0d40d234d324

Title: Suspicious Process Writes Ntds.dit
- description: Detects suspicious processes that write (copy) a Active Directory database (ntds.dit) file
- category: data/rules/windows/file_event
- level: high
- id: 11b1ed55-154d-4e82-8ad7-83739298f720

Title: UAC Bypass Using IEInstal - File
- description: Detects the pattern of UAC Bypass using IEInstal.exe (UACMe 64)
- category: data/rules/windows/file_event
- level: high
- id: bdd8157d-8e85-4397-bb82-f06cc9c71dbb

Title: Creation of an Executable by an Executable
- description: Detects the creation of an executable by another executable
- category: data/rules/windows/file_event
- level: low
- id: 297afac9-5d02-4138-8c58-b977bac60556

Title: QuarksPwDump Dump File
- description: Detects a dump file written by QuarksPwDump password dumper
- category: data/rules/windows/file_event
- level: critical
- id: 847def9e-924d-4e90-b7c4-5f581395a2b4

Title: Suspicious Creation with Colorcpl
- description: Once executed, colorcpl.exe will copy the arbitrary file to c:\windows\system32\spool\drivers\color\
- category: data/rules/windows/file_event
- level: high
- id: e15b518d-b4ce-4410-a9cd-501f23ce4a18

Title: Adwind RAT / JRAT
- description: Detects javaw.exe in AppData folder as used by Adwind / JRAT
- category: data/rules/windows/file_event
- level: high
- id: 0bcfabcb-7929-47f4-93d6-b33fb67d34d1

Title: Executable in ADS
- description: Detects the creation of an ADS data stream that contains an executable (non-empty imphash)
- category: data/rules/windows/create_stream_hash
- level: critical
- id: b69888d4-380c-45ce-9cf9-d9ce46e67821

Title: Exports Registry Key To an Alternate Data Stream
- description: Exports the target Registry key and hides it in the specified alternate data stream.
- category: data/rules/windows/create_stream_hash
- level: high
- id: 0d7a9363-af70-4e7b-a3b7-1a176b7fbe84

Title: Accessing WinAPI in PowerShell. Code Injection
- description: Detecting Code injection with PowerShell in another process
- category: data/rules/windows/create_remote_thread
- level: high
- id: eeb2e3dc-c1f4-40dd-9bd5-149ee465ad50

Title: Suspicious Remote Thread Created
- description: Offensive tradecraft is switching away from using APIs like "CreateRemoteThread", however, this is still largel
- category: data/rules/windows/create_remote_thread
- level: high
- id: 66d31e5f-52d6-40a4-9615-002d3789a119

Title: Remote Thread Creation Ttdinject.exe Proxy
- description: Detects a remote thread creation of Ttdinject.exe used as proxy
- category: data/rules/windows/create_remote_thread
- level: high
- id: c15e99a3-c474-48ab-b9a7-84549a7a9d16

Title: CobaltStrike Process Injection
- description: Detects a possible remote threat creation with certain characteristics which are typical for Cobalt Strike beac
- category: data/rules/windows/create_remote_thread
- level: high
- id: 6309645e-122d-4c5b-bb2b-22e4f9c2fa42

Title: Remote Thread Creation in Suspicious Targets
- description: Detects a remote thread creation in suspicious taregt images
- category: data/rules/windows/create_remote_thread
- level: high
- id: a1a144b7-5c9b-4853-a559-2172be8d4a03

Title: KeePass Password Dumping
- description: Detects remote thread creation in KeePass.exe indicating password dumping activity
- category: data/rules/windows/create_remote_thread
- level: high
- id: 77564cc2-7382-438b-a7f6-395c2ae53b9a

Title: PowerShell Rundll32 Remote Thread Creation
- description: Detects PowerShell remote thread creation in Rundll32.exe

- category: data/rules/windows/create_remote_thread
- level: high
- id: 99b97608-3e21-4bfe-8217-2a127c396a0e

Title: Password Dumper Remote Thread in LSASS
- description: Detects password dumper activity by monitoring remote thread creation EventID 8 in combination with the lsass.e
- category: data/rules/windows/create_remote_thread
- level: high
- id: f239b326-2f41-4d6b-9dfa-c846a60ef505

Title: CreateRemoteThread API and LoadLibrary
- description: Detects potential use of CreateRemoteThread api and LoadLibrary function to inject DLL into a process
- category: data/rules/windows/create_remote_thread
- level: critical
- id: 052ec6f6-1adc-41e6-907a-f1c813478bee

Title: CACTUSTORCH Remote Thread Creation
- description: Detects remote thread creation from CACTUSTORCH as described in references.
- category: data/rules/windows/create_remote_thread
- level: high
- id: 2e4e488a-6164-4811-9ea1-f960c7359c40

Title: Rename Common File to DLL File
- description: Detects cases in which a file gets renamed to .dll, which often happens to bypass perimeter protection
- category: data/rules/windows/file_rename
- level: medium
- id: bbfd974c-248e-4435-8de6-1e938c79c5c1

Title: Windows Registry Persistence COM Key Linking
- description: Detects COM object hijacking via TreatAs subkey
- category: data/rules/windows/registry/registry_add
- level: medium
- id: 9b0f8a61-91b2-464f-aceb-0527e0a45020

Title: Usage of Sysinternals Tools
- description: Detects the usage of Sysinternals Tools due to accepteula key being added to Registry
- category: data/rules/windows/registry/registry_add
- level: low
- id: 25ffa65d-76d8-4da5-a832-3f2b0136e133

Title: Sysinternals SDelete Registry Keys
- description: A General detection to trigger for the creation or modification of .*\Software\Sysinternals\SDelete registry ke
- category: data/rules/windows/registry/registry_add
- level: medium
- id: 9841b233-8df8-4ad7-9133-b0b4402a9014

Title: Logon Scripts Creation in UserInitMprLogonScript Registry
- description: Detects creation of UserInitMprLogonScript persistence method
- category: data/rules/windows/registry/registry_add
- level: high
- id: 9ace0707-b560-49b8-b6ca-5148b42f39fb

Title: Ursnif
- description: Detects new registry key created by Ursnif malware.
- category: data/rules/windows/registry/registry_add
- level: critical
- id: 21f17060-b282-4249-ade0-589ea3591558

Title: NetWire RAT Registry Key
- description: Attempts to detect registry events for common NetWire key HKCU\Software\NetWire
- category: data/rules/windows/registry/registry_add
- level: high
- id: 1d218616-71b0-4c40-855b-9dbe75510f7f

Title: Removal of Potential COM Hijacking Registry Keys
- description: A General detection to trigger for processes removing .*\shell\open\command registry keys. Registry keys that m
- category: data/rules/windows/registry/registry_delete
- level: medium
- id: 96f697b0-b499-4e5d-9908-a67bec11cdb6

Title: Removal Amsi Provider Reg Key
- description: Remove the AMSI Provider registry key in HKLM\Software\Microsoft\AMSI to disable AMSI inspection
- category: data/rules/windows/registry/registry_delete
- level: high
- id: 41d1058a-aea7-4952-9293-29eaaf516465

Title: Terminal Server Client Connection History Cleared
- description: Detects the deletion of registry keys containing the MSTSC connection history
- category: data/rules/windows/registry/registry_delete
- level: high
- id: 07bdd2f5-9c58-4f38-aec8-e101bb79ef8d

Title: Removal SD Value to Hide Schedule Task
- description: Remove SD (Security Descriptor) value in \Schedule\TaskCache\Tree registry hive to hide schedule task. This tec
- category: data/rules/windows/registry/registry_delete
- level: medium
- id: acd74772-5f88-45c7-956b-6a7b36c294d2

Title: Suspicious Service Installed
- description: Detects installation of NalDrv or PROCEXP152 services via registry-keys to non-system32 folders. Both services
- category: data/rules/windows/registry/registry_set
- level: medium
- id: f2485272-a156-4773-82d7-1d178bc4905b

Title: Disable PUA Protection on Windows Defender
- description: Detects disabling Windows Defender PUA protection
- category: data/rules/windows/registry/registry_set
- level: high
- id: 8ffc5407-52e3-478f-9596-0a7371eafe13

Title: Blackbyte Ransomware Registry
- description: BlackByte set three different registry values to escalate privileges and begin setting the stage for lateral mo
- category: data/rules/windows/registry/registry_set
- level: high
- id: 83314318-052a-4c90-a1ad-660ece38d276

Title: Running Chrome VPN Extensions via the Registry 2 VPN Extension
- description: Running Chrome VPN Extensions via the Registry install 2 vpn extension
- category: data/rules/windows/registry/registry_set
- level: high
- id: b64a026b-8deb-4c1d-92fd-98893209dff1

Title: Office Autorun Keys Modification
- description: Detects modification of autostart extensibility point (ASEP) in registry.
- category: data/rules/windows/registry/registry_set
- level: medium
- id: baecf8fb-edbf-429f-9ade-31fc3f22b970

Title: PowerShell Logging Disabled
- description: Detects the modification of the registry of the currently logged in user to disable PowerShell module logging,
- category: data/rules/windows/registry/registry_set
- level: medium
- id: fecfd1a1-cc78-4313-a1ea-2ee2e8ec27a7

Title: Disable Tamper Protection on Windows Defender
- description: Detects disabling Windows Defender Tamper Protection
- category: data/rules/windows/registry/registry_set
- level: medium
- id: 93d298a1-d28f-47f1-a468-d971e7796679

Title: Enable Microsoft Dynamic Data Exchange
- description: Enable Dynamic Data Exchange protocol (DDE) in all supported editions of Microsoft Word or Excel.
- category: data/rules/windows/registry/registry_set
- level: medium
- id: 63647769-326d-4dde-a419-b925cc0caf42

Title: Suspicious Printer Driver Empty Manufacturer
- description: Detects a suspicious printer driver installation with an empty Manufacturer value

- category: data/rules/windows/registry/registry_set
- level: high
- id: e0813366-0407-449a-9869-a2db1119dc41

Title: Stealthy VSTO Persistence
- description: Detects persistence via Visual Studio Tools for Office (VSTO) add-ins in Office applications.
- category: data/rules/windows/registry/registry_set
- level: medium
- id: 9d15044a-7cfe-4d23-8085-6ebc11df7685

Title: Service Binary in Uncommon Folder
- description: Detect the creation of a service with a service binary located in a uncommon directory
- category: data/rules/windows/registry/registry_set
- level: medium
- id: 277dc340-0540-42e7-8efb-5ff460045e07

Title: Changing RDP Port to Non Standard Number
- description: Remote desktop is a common feature in operating systems.

It allows a user to log into an interactive session with a system desktop graphical user interface on a remote system. Microsoft refers to its implementation of the Remote Desktop Protocol (RDP) as Remote Desktop Services (RDS).

- category: data/rules/windows/registry/registry_set
- level: high
- id: 509e84b9-a71a-40e0-834f-05470369bd1e

Title: GlobalFlags Registry Persistence Mechanisms
- description: Detects persistence registry keys
- category: data/rules/windows/registry/registry_set
- level: critical
- id: 36803969-5421-41ec-b92f-8500f79c23b0

Title: Session Manager Autorun Keys Modification
- description: Detects modification of autostart extensibility point (ASEP) in registry.
- category: data/rules/windows/registry/registry_set
- level: medium
- id: 046218bd-e0d8-4113-a3c3-895a12b2b298

Title: Registry Persitence via Service in Safe Mode
- description: Detects the modification of the registry to allow a driver or service to persist in Safe Mode.
- category: data/rules/windows/registry/registry_set
- level: high
- id: 1547e27c-3974-43e2-a7d7-7f484fb928ec

Title: Registry Disable System Restore
- description: Detects the modification of the registry to disable a system restore on the computer
- category: data/rules/windows/registry/registry_set
- level: high
- id: 5de03871-5d46-4539-a82d-3aa992a69a83

Title: Disable Microsoft Office Security Features
- description: Disable Microsoft Office Security Features by registry
- category: data/rules/windows/registry/registry_set
- level: high
- id: 7c637634-c95d-4bbf-b26c-a82510874b34

Title: Registry Hide Function from User
- description: Detects registry modifications that hide internal tools or functions from the user (malware like Agent Tesla, H
- category: data/rules/windows/registry/registry_set
- level: medium
- id: 5a93eb65-dffa-4543-b761-94aa60098fb6

Title: Service Binary in Temp Folder
- description: Detect the creation of a service with a service binary located in a temporary directory
- category: data/rules/windows/registry/registry_set
- level: high
- id: c0abc838-36b0-47c9-b3b3-a90c39455382

Title: Internet Explorer Autorun Keys Modification

- description: Detects modification of autostart extensibility point (ASEP) in registry.
- category: data/rules/windows/registry/registry_set
- level: medium
- id: a80f662f-022f-4429-9b8c-b1a41aaa6688

Title: Disable Microsoft Defender Firewall via Registry
- description: Adversaries may disable or modify system firewalls in order to bypass controls limiting network usage
- category: data/rules/windows/registry/registry_set
- level: medium
- id: 974515da-6cc5-4c95-ae65-f97f9150ec7f

Title: COMPlus_ETWEnabled Registry Modification
- description: Potential adversaries stopping ETW providers recording loaded .NET assemblies.
- category: data/rules/windows/registry/registry_set
- level: critical
- id: bf4fc428-dcc3-4bbd-99fe-2422aeee2544

Title: Wow6432Node CurrentVersion Autorun Keys Modification
- description: Detects modification of autostart extensibility point (ASEP) in registry.
- category: data/rules/windows/registry/registry_set
- level: medium
- id: 480421f9-417f-4d3b-9552-fd2728443ec8

Title: UAC Bypass via Sdclt
- description: Detects the pattern of UAC Bypass using registry key manipulation of sdclt.exe (e.g. UACMe 53)
- category: data/rules/windows/registry/registry_set
- level: high
- id: 5b872a46-3b90-45c1-8419-f675db8053aa

Title: Suspicious New Printer Ports in Registry (CVE-2020-1048)
- description: Detects a new and suspicious printer port creation in Registry that could be an attempt to exploit CVE-2020-104
- category: data/rules/windows/registry/registry_set
- level: high
- id: 7ec912f2-5175-4868-b811-ec13ad0f8567

Title: Registry Modification to Hidden File Extension
- description: Hides the file extension through modification of the registry
- category: data/rules/windows/registry/registry_set
- level: medium
- id: 5df86130-4e95-4a54-90f7-26541b40aec2

Title: UAC Bypass via Event Viewer
- description: Detects UAC bypass method using Windows event viewer
- category: data/rules/windows/registry/registry_set
- level: critical
- id: 7c81fec3-1c1d-43b0-996a-46753041b1b6

Title: Winlogon Notify Key Logon Persistence
- description: Adversaries may abuse features of Winlogon to execute DLLs and/or executables when a user logs in.

Winlogon.exe is a Windows component responsible for actions at logon/logoff as well as the secure attention sequence (SAS) triggered by Ctrl-Alt-Delete.

- category: data/rules/windows/registry/registry_set
- level: high
- id: bbf59793-6efb-4fa1-95ca-a7d288e52c88

Title: WinSock2 Autorun Keys Modification
- description: Detects modification of autostart extensibility point (ASEP) in registry.
- category: data/rules/windows/registry/registry_set
- level: medium
- id: d6c2ce7e-afb5-4337-9ca4-4b5254ed0565

Title: Registry Key Creation or Modification for Shim DataBase
- description: Adversaries may establish persistence and/or elevate privileges by executing malicious content triggered by app

The Microsoft Windows Application Compatibility Infrastructure/Framework (Application Shim) was created to allow for backward compatibility of software as the operating system codebase changes over time

- category: data/rules/windows/registry/registry_set
- level: medium

- id: dfb5b4e8-91d0-4291-b40a-e3b0d3942c45

Title: Windows Defender Real-Time Protection Disabled
- description: Detects disabling Windows Defender Real-Time Protection by modifying registry
- category: data/rules/windows/registry/registry_set
- level: high
- id: fd115e64-97c7-491f-951c-fc8da7e042fa

Title: Wdigest Enable UseLogonCredential
- description: Detects potential malicious modification of the property value of UseLogonCredential from HKLM:\SYSTEM\CurrentC
- category: data/rules/windows/registry/registry_set
- level: high
- id: d6a9b252-c666-4de6-8806-5561bbbd3bdc

Title: UAC Bypass Abusing Winsat Path Parsing - Registry
- description: Detects the pattern of UAC Bypass using a path parsing issue in winsat.exe (UACMe 52)
- category: data/rules/windows/registry/registry_set
- level: high
- id: 6597be7b-ac61-4ac8-bef4-d3ec88174853

Title: Bypass UAC Using SilentCleanup Task
- description: There is an auto-elevated task called SilentCleanup located in %windir%\system32\cleanmgr.exe This can be abuse
- category: data/rules/windows/registry/registry_set
- level: high
- id: 724ea201-6514-4f38-9739-e5973c34f49a

Title: Disable Exploit Guard Network Protection on Windows Defender
- description: Detects disabling Windows Defender Exploit Guard Network Protection
- category: data/rules/windows/registry/registry_set
- level: medium
- id: bf9e1387-b040-4393-9851-1598f8ecfae9

Title: IE Change Domain Zone
- description: Hides the file extension through modification of the registry
- category: data/rules/windows/registry/registry_set
- level: medium
- id: 45e112d0-7759-4c2a-aa36-9f8fb79d3393

Title: Office Security Settings Changed
- description: Detects registry changes to Office macro settings. The TrustRecords contain information on executed macro-enabl
- category: data/rules/windows/registry/registry_set
- level: high
- id: a166f74e-bf44-409d-b9ba-ea4b2dd8b3cd

Title: Modification of IE Registry Settings
- description: Detects the modification of the registry settings used for Internet Explorer and other Windows components that
- category: data/rules/windows/registry/registry_set
- level: low
- id: d88d0ab2-e696-4d40-a2ed-9790064e66b3

Title: ServiceDll Modification
- description: Detects the modification of a ServiceDLL value in the service settings
- category: data/rules/windows/registry/registry_set
- level: medium
- id: 612e47e9-8a59-43a6-b404-f48683f45bd6

Title: CurrentVersion NT Autorun Keys Modification
- description: Detects modification of autostart extensibility point (ASEP) in registry.
- category: data/rules/windows/registry/registry_set
- level: medium
- id: cbf93e5d-ca6c-4722-8bea-e9119007c248

Title: CobaltStrike Service Installations in Registry
- description: Detects known malicious service installs that appear in cases in which a Cobalt Strike beacon elevates privileg
- category: data/rules/windows/registry/registry_set
- level: critical
- id: 61a7697c-cb79-42a8-a2ff-5f0cdfae0130

Title: Execution DLL of Choice Using WAB.EXE

- description: This rule detects that the path to the DLL written in the registry is different from the default one. Launched
- category: data/rules/windows/registry/registry_set
- level: high
- id: fc014922-5def-4da9-a0fc-28c973f41bfb

Title: Outlook C2 Registry Key
- description: Detects the modification of Outlook Security Setting to allow unprompted execution. Goes with win_outlook_c2_ma
- category: data/rules/windows/registry/registry_set
- level: medium
- id: e3b50fa5-3c3f-444e-937b-0a99d33731cd

Title: New RUN Key Pointing to Suspicious Folder
- description: Detects suspicious new RUN key element pointing to an executable in a suspicious folder
- category: data/rules/windows/registry/registry_set
- level: high
- id: 02ee49e2-e294-4d0f-9278-f5b3212fc588

Title: New File Association Using Exefile
- description: Detects the abuse of the exefile handler in new file association. Used for bypass of security products.
- category: data/rules/windows/registry/registry_set
- level: high
- id: 44a22d59-b175-4f13-8c16-cbaef5b581ff

Title: New Application in AppCompat
- description: A General detection for a new application in AppCompat. This indicates an application executing for the first t
- category: data/rules/windows/registry/registry_set
- level: informational
- id: 60936b49-fca0-4f32-993d-7415edcf9a5d

Title: Service Binary in Suspicious Folder
- description: Detect the creation of a service with a service binary located in a suspicious directory
- category: data/rules/windows/registry/registry_set
- level: high
- id: a07f0359-4c90-4dc4-a681-8ffea40b4f47

Title: Common Autorun Keys Modification
- description: Detects modification of autostart extensibility point (ASEP) in registry.
- category: data/rules/windows/registry/registry_set
- level: medium
- id: f59c3faf-50f3-464b-9f4c-1b67ab512d99

Title: RDP Registry Modification
- description: Detects potential malicious modification of the property value of fDenyTSConnections and UserAuthentication to
- category: data/rules/windows/registry/registry_set
- level: high
- id: 41904ebe-d56c-4904-b9ad-7a77bdf154b3

Title: Adwind RAT / JRAT
- description: Detects javaw.exe in AppData folder as used by Adwind / JRAT
- category: data/rules/windows/registry/registry_set
- level: high
- id: 42f0e038-767e-4b85-9d96-2c6335bad0b5

Title: Windows Registry Persistence COM Search Order Hijacking
- description: Detects potential COM object hijacking leveraging the COM Search Order
- category: data/rules/windows/registry/registry_set
- level: medium
- id: a0ff33d8-79e4-4cef-b4f3-9dc4133ccd12

Title: Scheduled TaskCache Change by Uncommon Program
- description: Monitor the creation of a new key under 'TaskCache' when a new scheduled task is registered by a process that i
- category: data/rules/windows/registry/registry_set
- level: high
- id: 4720b7df-40c3-48fd-bbdf-fd4b3c464f0d

Title: Wow6432Node CurrentVersion Autorun Keys Modification
- description: Detects modification of autostart extensibility point (ASEP) in registry.
- category: data/rules/windows/registry/registry_set
- level: medium

- id: b29aed60-ebd1-442b-9cb5-16a1d0324adb

Title: CurrentVersion Autorun Keys Modification
- description: Detects modification of autostart extensibility point (ASEP) in registry.
- category: data/rules/windows/registry/registry_set
- level: medium
- id: 20f0ee37-5942-4e45-b7d5-c5b5db9df5cd

Title: Suspicious Keyboard Layout Load
- description: Detects the keyboard preload installation with a suspicious keyboard layout, e.g. Chinese, Iranian or Vietnames
- category: data/rules/windows/registry/registry_set
- level: medium
- id: 34aa0252-6039-40ff-951f-939fd6ce47d8

Title: UAC Bypass Using Windows Media Player - Registry
- description: Detects the pattern of UAC Bypass using Windows Media Player osksupport.dll (UACMe 32)
- category: data/rules/windows/registry/registry_set
- level: high
- id: 5f9db380-ea57-4d1e-beab-8a2d33397e93

Title: New Root or CA or AuthRoot Certificate to Store
- description: Detects the addition of new root, CA or AuthRoot certificates to the Windows registry
- category: data/rules/windows/registry/registry_set
- level: medium
- id: d223b46b-5621-4037-88fe-fda32eead684

Title: PowerShell as a Service in Registry
- description: Detects that a powershell code is written to the registry as a service.
- category: data/rules/windows/registry/registry_set
- level: high
- id: 4a5f5a5e-ac01-474b-9b4e-d61298c9df1d

Title: Persistent Outlook Landing Pages
- description: Detects the manipulation of persistent URLs which could execute malicious code
- category: data/rules/windows/registry/registry_set
- level: high
- id: 487bb375-12ef-41f6-baae-c6a1572b4dd1

Title: Powershell in Windows Run Keys
- description: Adds a RUN key that contains a powershell keyword
- category: data/rules/windows/registry/registry_set
- level: medium
- id: 8d85cf08-bf97-4260-ba49-986a2a65129c

Title: Windows Defender Exclusions Added
- description: Detects the Setting of Windows Defender Exclusions
- category: data/rules/windows/registry/registry_set
- level: medium
- id: a982fc9c-6333-4ffb-a51d-addb04e8b529

Title: Registry Explorer Policy Modification
- description: Detects registry modifications that disable internal tools or functions in explorer (malware like Agent Tesla u
- category: data/rules/windows/registry/registry_set
- level: medium
- id: 1c3121ed-041b-4d97-a075-07f54f20fb4a

Title: DHCP Callout DLL Installation
- description: Detects the installation of a Callout DLL via CalloutDlls and CalloutEnabled parameter in Registry, which can b
- category: data/rules/windows/registry/registry_set
- level: high
- id: 9d3436ef-9476-4c43-acca-90ce06bdf33a

Title: Disable Administrative Share Creation at Startup
- description: Administrative shares are hidden network shares created by Microsoft’s Windows NT operating systems that grant
- category: data/rules/windows/registry/registry_set
- level: medium
- id: c7dcacd0-cc59-4004-b0a4-1d6cdebe6f3e

Title: System Scripts Autorun Keys Modification

- description: Detects modification of autostart extensibility point (ASEP) in registry.
- category: data/rules/windows/registry/registry_set
- level: medium
- id: e7a2fd40-3ae1-4a85-bf80-15cf624fb1b1

Title: CurrentControlSet Autorun Keys Modification
- description: Detects modification of autostart extensibility point (ASEP) in registry.
- category: data/rules/windows/registry/registry_set
- level: medium
- id: f674e36a-4b91-431e-8aef-f8a96c2aca35

Title: Registry Persistence Mechanism via Windows Telemetry
- description: Detects persistence method using windows telemetry
- category: data/rules/windows/registry/registry_set
- level: critical
- id: 73a883d0-0348-4be4-a8d8-51031c2564f8

Title: DNS-over-HTTPS Enabled by Registry
- description: Detects when a user enables DNS-over-HTTPS. This can be used to hide internet activity or be used to hide the p
- category: data/rules/windows/registry/registry_set
- level: medium
- id: 04b45a8a-d11d-49e4-9acc-4a1b524407a5

Title: Change Outlook Security Setting in Registry
- description: Change outlook email security settings
- category: data/rules/windows/registry/registry_set
- level: medium
- id: c3cefdf4-6703-4e1c-bad8-bf422fc5015a

Title: Persistent Outlook Landing Pages
- description: Detects the manipulation of persistent URLs which can be malicious
- category: data/rules/windows/registry/registry_set
- level: high
- id: ddd171b5-2cc6-4975-9e78-f0eccd08cc76

Title: Add Port Monitor Persistence in Registry
- description: Adversaries may use port monitors to run an attacker supplied DLL during system boot for persistence or privile

A port monitor can be set through the AddMonitor API call to set a DLL to be loaded at startup.

- category: data/rules/windows/registry/registry_set
- level: high
- id: 944e8941-f6f6-4ee8-ac05-1c224e923c0e

Title: Bypass UAC Using DelegateExecute
- description: Bypasses User Account Control using a fileless method
- category: data/rules/windows/registry/registry_set
- level: high
- id: 46dd5308-4572-4d12-aa43-8938f0184d4f

Title: Enabling COR Profiler Environment Variables
- description: This rule detects cor_enable_profiling and cor_profiler environment variables being set and configured.
- category: data/rules/windows/registry/registry_set
- level: high
- id: ad89044a-8f49-4673-9a55-cbd88a1b374f

Title: ScreenSaver Registry Key Set
- description: Detects registry key established after masqueraded .scr file execution using Rundll32 through desk.cpl
- category: data/rules/windows/registry/registry_set
- level: medium
- id: 40b6e656-4e11-4c0c-8772-c1cc6dae34ce

Title: Blue Mockingbird
- description: Attempts to detect system changes made by Blue Mockingbird
- category: data/rules/windows/registry/registry_set
- level: high
- id: 92b0b372-a939-44ed-a11b-5136cf680e27

Title: Windows Defender Threat Detection Disabled - Registry

- description: Detects disabling Windows Defender threat protection
- category: data/rules/windows/registry/registry_set
- level: high
- id: a64e4198-c1c8-46a5-bc9c-324c86455fd4

Title: VBScript Payload Stored in Registry
- description: Detects VBScript content stored into registry keys as seen being used by UNC2452 group
- category: data/rules/windows/registry/registry_set
- level: high
- id: 46490193-1b22-4c29-bdd6-5bf63907216f

Title: Classes Autorun Keys Modification
- description: Detects modification of autostart extensibility point (ASEP) in registry.
- category: data/rules/windows/registry/registry_set
- level: medium
- id: 9df5f547-c86a-433e-b533-f2794357e242

Title: Registry Persistence via Explorer Run Key
- description: Detects a possible persistence mechanism using RUN key for Windows Explorer and pointing to a suspicious folder
- category: data/rules/windows/registry/registry_set
- level: high
- id: b7916c2a-fa2f-4795-9477-32b731f70f11

Title: RDP Sensitive Settings Changed
- description: Detects changes to RDP terminal service sensitive settings
- category: data/rules/windows/registry/registry_set
- level: high
- id: 171b67e1-74b4-460e-8d55-b331f3e32d67

Title: Wow6432Node Classes Autorun Keys Modification
- description: Detects modification of autostart extensibility point (ASEP) in registry.
- category: data/rules/windows/registry/registry_set
- level: medium
- id: 18f2065c-d36c-464a-a748-bcf909acb2e3

Title: Disable Internal Tools or Feature in Registry
- description: Detects registry modifications that change features of internal Windows tools (malware like Agent Tesla uses th
- category: data/rules/windows/registry/registry_set
- level: medium
- id: e2482f8d-3443-4237-b906-cc145d87a076

Title: Modification of Explorer Hidden Keys
- description: Detects modifications to the hidden files keys in registry. This technique is abused by several malware familie
- category: data/rules/windows/registry/registry_set
- level: medium
- id: 5a5152f1-463f-436b-b2f5-8eceb3964b42

Title: SilentProcessExit Monitor Registrytion
- description: Detects changes to the Registry in which a monitor program gets registered to monitor the exit of another proce
- category: data/rules/windows/registry/registry_set
- level: high
- id: c81fe886-cac0-4913-a511-2822d72ff505

Title: Bypass UAC Using Event Viewer
- description: Bypasses User Account Control using Event Viewer and a relevant Windows Registry modification
- category: data/rules/windows/registry/registry_set
- level: high
- id: 674202d0-b22a-4af4-ae5f-2eda1f3da1af

Title: Disable UAC Using Registry
- description: Disable User Account Conrol (UAC) by changing its registry key HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\P
- category: data/rules/windows/registry/registry_set
- level: medium
- id: 48437c39-9e5f-47fb-af95-3d663c3f2919

Title: COM Hijack via Sdclt
- description: Detects changes to 'HKCU\Software\Classes\Folder\shell\open\command\DelegateExecute'
- category: data/rules/windows/registry/registry_set
- level: high

- id: 07743f65-7ec9-404a-a519-913db7118a8d

Title: Abusing Windows Telemetry For Persistence
- description: Windows telemetry makes use of the binary CompatTelRunner.exe to run a variety of commands and perform the actu
- category: data/rules/windows/registry/registry_set
- level: high
- id: 4e8d5fd3-c959-441f-a941-f73d0cdcdca5

Title: Pandemic Registry Key
- description: Detects Pandemic Windows Implant
- category: data/rules/windows/registry/registry_event
- level: critical
- id: 47e0852a-cf81-4494-a8e6-31864f8c86ed

Title: Registry Persistence Mechanisms in Recycle Bin
- description: Detects persistence registry keys for Recycle Bin
- category: data/rules/windows/registry/registry_event
- level: critical
- id: 277efb8f-60be-4f10-b4d3-037802f37167

Title: Leviathan Registry Key Activity
- description: Detects registry key used by Leviathan APT in Malaysian focused campaign
- category: data/rules/windows/registry/registry_event
- level: critical
- id: 70d43542-cd2d-483c-8f30-f16b436fd7db

Title: WINEKEY Registry Modification
- description: Detects potential malicious modification of run keys by winekey or team9 backdoor
- category: data/rules/windows/registry/registry_event
- level: high
- id: b98968aa-dbc0-4a9c-ac35-108363cbf8d5

Title: PortProxy Registry Key
- description: Detects the modification of PortProxy registry key which is used for port forwarding. For command execution see
- category: data/rules/windows/registry/registry_event
- level: medium
- id: a54f842a-3713-4b45-8c84-5f136fdebd3c

Title: DNS ServerLevelPluginDll Install
- description: Detects the installation of a plugin DLL via ServerLevelPluginDll parameter in Registry, which can be used to e
- category: data/rules/windows/registry/registry_event
- level: high
- id: e61e8a88-59a9-451c-874e-70fcc9740d67

Title: Path To Screensaver Binary Modified
- description: Detects value modification of registry key containing path to binary used as screensaver.
- category: data/rules/windows/registry/registry_event
- level: medium
- id: 67a6c006-3fbe-46a7-9074-2ba3b82c3000

Title: CrashControl CrashDump Disabled
- description: Detects disabling the CrashDump per registry (as used by HermeticWiper)
- category: data/rules/windows/registry/registry_event
- level: medium
- id: 2ff692c2-4594-41ec-8fcb-46587de769e0

Title: DLL Load via LSASS
- description: Detects a method to load DLL via LSASS process using an undocumented Registry key
- category: data/rules/windows/registry/registry_event
- level: high
- id: b3503044-60ce-4bf4-bbcb-e3db98788823

Title: New DLL Added to AppCertDlls Registry Key
- description: Dynamic-link libraries (DLLs) that are specified in the AppCertDLLs value in the Registry key can be abused to
- category: data/rules/windows/registry/registry_event
- level: medium
- id: 6aa1d992-5925-4e9f-a49b-845e51d1de01

Title: RedMimicry Winnti Playbook Registry Manipulation

- description: Detects actions caused by the RedMimicry Winnti playbook
- category: data/rules/windows/registry/registry_event
- level: high
- id: 5b175490-b652-4b02-b1de-5b5b4083c5f8

Title: OceanLotus Registry Activity
- description: Detects registry keys created in OceanLotus (also known as APT32) attacks
- category: data/rules/windows/registry/registry_event
- level: critical
- id: 4ac5fc44-a601-4c06-955b-309df8c4e9d4

Title: FlowCloud Malware
- description: Detects FlowCloud malware from threat group TA410.
- category: data/rules/windows/registry/registry_event
- level: critical
- id: 5118765f-6657-4ddb-a487-d7bd673abbf1

Title: Chafer Activity
- description: Detects Chafer activity attributed to OilRig as reported in Nyotron report in March 2018
- category: data/rules/windows/registry/registry_event
- level: critical
- id: 7bdf2a7c-3acc-4091-9581-0a77dad1c5b5

Title: Windows Credential Editor Registry
- description: Detects the use of Windows Credential Editor (WCE)
- category: data/rules/windows/registry/registry_event
- level: critical
- id: a6b33c02-8305-488f-8585-03cb2a7763f2

Title: Run Once Task Configuration in Registry
- description: Rule to detect the configuration of Run Once registry key. Configured payload can be run by runonce.exe /Altern
- category: data/rules/windows/registry/registry_event
- level: medium
- id: c74d7efc-8826-45d9-b8bb-f04fac9e4eff

Title: NetNTLM Downgrade Attack
- description: Detects NetNTLM downgrade attack
- category: data/rules/windows/registry/registry_event
- level: critical
- id: d67572a0-e2ec-45d6-b8db-c100d14b8ef2

Title: Wdigest CredGuard Registry Modification
- description: Detects potential malicious modification of the property value of IsCredGuardEnabled from HKLM:\SYSTEM\CurrentC
- category: data/rules/windows/registry/registry_event
- level: critical
- id: 1a2d6c47-75b0-45bd-b133-2c0be75349fd

Title: New DLL Added to AppInit_DLLs Registry Key
- description: DLLs that are specified in the AppInit_DLLs value in the Registry key HKLM\Software\Microsoft\Windows NT\Curren
- category: data/rules/windows/registry/registry_event
- level: medium
- id: 4f84b697-c9ed-4420-8ab5-e09af5b2345d

Title: Sticky Key Like Backdoor Usage
- description: Detects the usage and installation of a backdoor that uses an option to register a malicious debugger for built
- category: data/rules/windows/registry/registry_event
- level: critical
- id: baca5663-583c-45f9-b5dc-ea96a22ce542

Title: Narrator's Feedback-Hub Persistence
- description: Detects abusing Windows 10 Narrator's Feedback-Hub
- category: data/rules/windows/registry/registry_event
- level: high
- id: f663a6d9-9d1b-49b8-b2b1-0637914d199a

Title: Creation of a Local Hidden User Account by Registry
- description: Sysmon registry detection of a local hidden user account.
- category: data/rules/windows/registry/registry_event
- level: high

- id: 460479f3-80b7-42da-9c43-2cc1d54dbccd

Title: Atbroker Registry Change
- description: Detects creation/modification of Assisitive Technology applications and persistence with usage of ATs
- category: data/rules/windows/registry/registry_event
- level: high
- id: 9577edbb-851f-4243-8c91-1d5b50c1a39b

Title: Suspicious Run Key from Download
- description: Detects the suspicious RUN keys created by software located in Download or temporary Outlook/Internet Explorer
- category: data/rules/windows/registry/registry_event
- level: high
- id: 9c5037d1-c568-49b3-88c7-9846a5bdc2be

Title: Windows Registry Trust Record Modification
- description: Alerts on trust record modification within the registry, indicating usage of macros
- category: data/rules/windows/registry/registry_event
- level: medium
- id: 295a59c1-7b79-4b47-a930-df12c15fc9c2

Title: Shell Open Registry Keys Manipulation
- description: Detects the shell open key manipulation (exefile and ms-settings) used for persistence and the pattern of UAC B
- category: data/rules/windows/registry/registry_event
- level: high
- id: 152f3630-77c1-4284-bcc0-4cc68ab2f6e7

Title: Suspicious Camera and Microphone Access
- description: Detects Processes accessing the camera and microphone from suspicious folder
- category: data/rules/windows/registry/registry_event
- level: high
- id: 62120148-6b7a-42be-8b91-271c04e281a3

Title: Registry Entries For Azorult Malware
- description: Detects the presence of a registry key created during Azorult execution
- category: data/rules/windows/registry/registry_event
- level: critical
- id: f7f9ab88-7557-4a69-b30e-0a8f91b3a0e7

Title: Office Application Startup - Office Test
- description: Detects the addition of office test registry that allows a user to specify an arbitrary DLL that will be execut
- category: data/rules/windows/registry/registry_event
- level: medium
- id: 3d27f6dd-1c74-4687-b4fa-ca849d128d1c

Title: Disable Security Events Logging Adding Reg Key MiniNt
- description: Detects the addition of a key 'MiniNt' to the registry. Upon a reboot, Windows Event Log service will stopped w
- category: data/rules/windows/registry/registry_event
- level: high
- id: 919f2ef0-be2d-4a7a-b635-eb2b41fde044

Title: UAC Bypass Via Wsreset
- description: Unfixed method for UAC bypass from windows 10. WSReset.exe file associated with the Windows Store. It will run
- category: data/rules/windows/registry/registry_event
- level: high
- id: 6ea3bf32-9680-422d-9f50-e90716b12a66

Title: CVE-2021-31979 CVE-2021-33771 Exploits by Sourgum
- description: Detects patterns as noticed in exploitation of Windows CVE-2021-31979 CVE-2021-33771 vulnerability and DevilsTo
- category: data/rules/windows/registry/registry_event
- level: critical
- id: 32b5db62-cb5f-4266-9639-0fa48376ac00

Title: Security Support Provider (SSP) Added to LSA Configuration
- description: Detects the addition of a SSP to the registry. Upon a reboot or API call, SSP DLLs gain access to encrypted and
- category: data/rules/windows/registry/registry_event
- level: critical
- id: eeb30123-9fbd-4ee8-aaa0-2e545bbed6dc

Title: PrinterNightmare Mimimkatz Driver Name

- description: Detects static QMS 810 and mimikatz driver name used by Mimikatz as exploited in CVE-2021-1675 and CVE-2021-345
- category: data/rules/windows/registry/registry_event
- level: critical
- id: ba6b9e43-1d45-4d3c-a504-1043a64c8469

Title: Esentutl Volume Shadow Copy Service Keys
- description: Detects the volume shadow copy service initialization and processing via esentutl. Registry keys such as HKLM\\
- category: data/rules/windows/registry/registry_event
- level: high
- id: 5aad0995-46ab-41bd-a9ff-724f41114971

Title: SilentProcessExit Monitor Registrytion for LSASS
- description: Detects changes to the Registry in which a monitor program gets registered to dump process memory of the lsass.
- category: data/rules/windows/registry/registry_event
- level: critical
- id: 55e29995-75e7-451a-bef0-6225e2f13597

Title: CMSTP Execution Registry Event
- description: Detects various indicators of Microsoft Connection Manager Profile Installer execution
- category: data/rules/windows/registry/registry_event
- level: high
- id: b6d235fc-1d38-4b12-adbe-325f06728f37

Title: HybridConnectionManager Service Installation
- description: Detects the installation of the Azure Hybrid Connection Manager service to allow remote code execution from Azu
- category: data/rules/windows/registry/registry_event
- level: high
- id: ac8866c7-ce44-46fd-8c17-b24acff96ca8

Title: Outgoing Logon with New Credentials
- description: Detects logon events that specify new credentials
- category: data/rules/windows/builtin
- level: low
- id: def8b624-e08f-4ae1-8612-1ba21190da6b

Title: Mimikatz Use
- description: This method detects mimikatz keywords in different Eventlogs (some of them only appear in older Mimikatz versio
- category: data/rules/windows/builtin
- level: critical
- id: 06d71506-7beb-4f22-8888-e2e5e2ca7fd8

Title: System Eventlog Cleared
- description: One of the Windows Core Eventlogs has been cleared. e.g. caused by "wevtutil cl" command execution
- category: data/rules/windows/builtin/system
- level: high
- id: 100ef69e-3327-481c-8e5c-6d80d9507556

Title: Invoke-Obfuscation RUNDLL LAUNCHER
- description: Detects Obfuscated Powershell via RUNDLL LAUNCHER
- category: data/rules/windows/builtin/system
- level: medium
- id: 11b52f18-aaec-4d60-9143-5dd8cc4706b9

Title: KrbRelayUp Service Installation
- description: Detects service creation from KrbRelayUp tool used for privilege escalation in windows domain environments wher
- category: data/rules/windows/builtin/system
- level: high
- id: e97d9903-53b2-41fc-8cb9-889ed4093e80

Title: Invoke-Obfuscation Via Use Rundll32
- description: Detects Obfuscated Powershell via use Rundll32 in Scripts
- category: data/rules/windows/builtin/system
- level: high
- id: 641a4bfb-c017-44f7-800c-2aee0184ce9b

Title: CobaltStrike Service Installations
- description: Detects known malicious service installs that appear in cases in which a Cobalt Strike beacon elevates privileg
- category: data/rules/windows/builtin/system
- level: critical

- id: 5a105d34-05fc-401e-8553-272b45c1522d

Title: Invoke-Obfuscation Obfuscated IEX Invocation
- description: Detects all variations of obfuscated powershell IEX invocation code generated by Invoke-Obfuscation framework f
- category: data/rules/windows/builtin/system
- level: high
- id: 51aa9387-1c53-4153-91cc-d73c59ae1ca9

Title: Invoke-Obfuscation COMPRESS OBFUSCATION
- description: Detects Obfuscated Powershell via COMPRESS OBFUSCATION
- category: data/rules/windows/builtin/system
- level: medium
- id: 175997c5-803c-4b08-8bb0-70b099f47595

Title: StoneDrill Service Install
- description: This method detects a service install of the malicious Microsoft Network Realtime Inspection Service service de
- category: data/rules/windows/builtin/system
- level: high
- id: 9e987c6c-4c1e-40d8-bd85-dd26fba8fdd6

Title: DHCP Server Loaded the CallOut DLL
- description: This rule detects a DHCP server in which a specified Callout DLL (in registry) was loaded
- category: data/rules/windows/builtin/system
- level: critical
- id: 13fc89a9-971e-4ca6-b9dc-aa53a445bf40

Title: Turla Service Install
- description: This method detects a service install of malicious services mentioned in Carbon Paper - Turla report by ESET
- category: data/rules/windows/builtin/system
- level: high
- id: 1df8b3da-b0ac-4d8a-b7c7-6cb7c24160e4

Title: Rare Service Installations
- description: Detects rare service installs that only appear a few times per time frame and could reveal password dumpers, ba
- category: data/rules/windows/builtin/system
- level: low
- id: 66bfef30-22a5-4fcd-ad44-8d81e60922ae

Title: Invoke-Obfuscation VAR++ LAUNCHER OBFUSCATION
- description: Detects Obfuscated Powershell via VAR++ LAUNCHER
- category: data/rules/windows/builtin/system
- level: high
- id: 14bcba49-a428-42d9-b943-e2ce0f0f7ae6

Title: Vulnerable Netlogon Secure Channel Connection Allowed
- description: Detects that a vulnerable Netlogon secure channel connection was allowed, which could be an indicator of CVE-20
- category: data/rules/windows/builtin/system
- level: high
- id: a0cb7110-edf0-47a4-9177-541a4083128a

Title: Windows Update Error
- description: Windows Update get some error Check if need a 0-days KB
- category: data/rules/windows/builtin/system
- level: low
- id: 13cfeb75-9e33-4d04-b0f7-ab8faaa95a59

Title: Invoke-Obfuscation VAR+ Launcher
- description: Detects Obfuscated use of Environment Variables to execute PowerShell
- category: data/rules/windows/builtin/system
- level: high
- id: 8ca7004b-e620-4ecb-870e-86129b5b8e75

Title: smbexec.py Service Installation
- description: Detects the use of smbexec.py tool by detecting a specific service installation
- category: data/rules/windows/builtin/system
- level: critical
- id: 52a85084-6989-40c3-8f32-091e12e13f09

Title: Volume Shadow Copy Mount

- description: Detects volume shadow copy mount
- category: data/rules/windows/builtin/system
- level: low
- id: f512acbf-e662-4903-843e-97ce4652b740

Title: Chafer Activity
- description: Detects Chafer activity attributed to OilRig as reported in Nyotron report in March 2018
- category: data/rules/windows/builtin/system
- level: critical
- id: 53ba33fd-3a50-4468-a5ef-c583635cfa92

Title: Suspicious Service Installation Script
- description: Detects suspicious service installation scripts
- category: data/rules/windows/builtin/system
- level: high
- id: 70f00d10-60b2-4f34-b9a0-dc3df3fe762a

Title: Exploit SamAccountName Spoofing with Kerberos
- description: The attacker creates a computer object using those permissions with a password known to her.

After that she clears the attribute ServicePrincipalName on the computer object. Because she created the object (CREATOR OWNER), she gets granted additional permissions and can do many changes to the object.

- category: data/rules/windows/builtin/system
- level: medium
- id: 44bbff3e-4ca3-452d-a49a-6efa4cafa06f

Title: SAM Dump to AppData
- description: Detects suspicious SAM dump activity as cause by QuarksPwDump and other password dumpers
- category: data/rules/windows/builtin/system
- level: high
- id: 839dd1e8-eda8-4834-8145-01beeee33acd

Title: Invoke-Obfuscation Via Use Clip
- description: Detects Obfuscated Powershell via use Clip.exe in Scripts
- category: data/rules/windows/builtin/system
- level: high
- id: 63e3365d-4824-42d8-8b82-e56810fefa0c

Title: Windows Pcap Drivers
- description: Detects Windows Pcap driver installation based on a list of associated .sys files.
- category: data/rules/windows/builtin/system
- level: medium
- id: 7b687634-ab20-11ea-bb37-0242ac130002

Title: Tap Driver Installation
- description: Well-known TAP software installation. Possible preparation for data exfiltration using tunnelling techniques
- category: data/rules/windows/builtin/system
- level: medium
- id: 8e4cf0e5-aa5d-4dc3-beff-dc26917744a9

Title: Meterpreter or Cobalt Strike Getsystem Service Installation
- description: Detects the use of getsystem Meterpreter/Cobalt Strike command by detecting a specific service installation
- category: data/rules/windows/builtin/system
- level: critical
- id: 843544a7-56e0-4dcc-a44f-5cc266dd97d6

Title: Potential RDP Exploit CVE-2019-0708
- description: Detect suspicious error on protocol RDP, potential CVE-2019-0708
- category: data/rules/windows/builtin/system
- level: medium
- id: aaa5b30d-f418-420b-83a0-299cb6024885

Title: Moriya Rootkit
- description: Detects the use of Moriya rootkit as described in the securelist's Operation TunnelSnake report
- category: data/rules/windows/builtin/system
- level: critical
- id: 25b9c01c-350d-4b95-bed1-836d04a4f324

Title: Turla PNG Dropper Service
- description: This method detects malicious services mentioned in Turla PNG dropper report by NCC Group in November 2018
- category: data/rules/windows/builtin/system
- level: critical
- id: 1228f8e2-7e79-4dea-b0ad-c91f1d5016c1

Title: Credential Dumping Tools Service Execution
- description: Detects well-known credential dumping tools execution via service execution events
- category: data/rules/windows/builtin/system
- level: high
- id: 4976aa50-8f41-45c6-8b15-ab3fc10e79ed

Title: Invoke-Obfuscation CLIP+ Launcher
- description: Detects Obfuscated use of Clip.exe to execute PowerShell
- category: data/rules/windows/builtin/system
- level: high
- id: f7385ee2-0e0c-11eb-adc1-0242ac120002

Title: ProcessHacker Privilege Elevation
- description: Detects a ProcessHacker tool that elevated privileges to a very high level
- category: data/rules/windows/builtin/system
- level: high
- id: c4ff1eac-84ad-44dd-a6fb-d56a92fc43a9

Title: Sysmon Crash
- description: Detectes application popup reporting a failure of the Sysmon service
- category: data/rules/windows/builtin/system
- level: high
- id: 4d7f1827-1637-4def-8d8a-fd254f9454df

Title: Zerologon Exploitation Using Well-known Tools
- description: This rule is designed to detect attempts to exploit Zerologon (CVE-2020-1472) vulnerability using mimikatz zero
- category: data/rules/windows/builtin/system
- level: critical
- id: 18f37338-b9bd-4117-a039-280c81f7a596

Title: Eventlog Cleared
- description: One of the Windows Eventlogs has been cleared. e.g. caused by "wevtutil cl" command execution
- category: data/rules/windows/builtin/system
- level: low
- id: a62b37e0-45d3-48d9-a517-90c1a1b0186b

Title: NTLMv1 Logon Between Client and Server
- description: Detects the reporting of NTLMv1 being used between a client and server
- category: data/rules/windows/builtin/system
- level: low
- id: e9d4ab66-a532-4ef7-a502-66a9e4a34f5d

Title: PowerShell Scripts Installed as Services
- description: Detects powershell script installed as a Service
- category: data/rules/windows/builtin/system
- level: high
- id: a2e5019d-a658-4c6a-92bf-7197b54e2cae

Title: QuarksPwDump Clearing Access History
- description: Detects QuarksPwDump clearing access history in hive
- category: data/rules/windows/builtin/system
- level: critical
- id: 39f919f3-980b-4e6f-a975-8af7e507ef2b

Title: Invoke-Obfuscation Via Stdin
- description: Detects Obfuscated Powershell via Stdin in Scripts
- category: data/rules/windows/builtin/system
- level: high
- id: 487c7524-f892-4054-b263-8a0ace63fc25

Title: Invoke-Obfuscation STDIN+ Launcher
- description: Detects Obfuscated use of stdin to execute PowerShell
- category: data/rules/windows/builtin/system

- level: high
- id: 72862bf2-0eb1-11eb-adc1-0242ac120002

Title: Suspicious Service Installation
- description: Detects suspicious service installation commands
- category: data/rules/windows/builtin/system
- level: high
- id: 1d61f71d-59d2-479e-9562-4ff5f4ead16b

Title: Windows Defender Threat Detection Disabled - Service
- description: Detects disabling Windows Defender threat protection
- category: data/rules/windows/builtin/system
- level: low
- id: 6c0a7755-6d31-44fa-80e1-133e57752680

Title: NTFS Vulnerability Exploitation
- description: This the exploitation of a NTFS vulnerability as reported without many details via Twitter
- category: data/rules/windows/builtin/system
- level: critical
- id: f14719ce-d3ab-4e25-9ce6-2899092260b0

Title: PsExec Tool Execution
- description: Detects PsExec service installation and execution events (service and Sysmon)
- category: data/rules/windows/builtin/system
- level: low
- id: 42c575ea-e41e-41f1-b248-8093c3e82a28

Title: Service Installation in Suspicious Folder
- description: Detects service installation in suspicious folder appdata
- category: data/rules/windows/builtin/system
- level: medium
- id: 5e993621-67d4-488a-b9ae-b420d08b96cb

Title: Invoke-Obfuscation Via Use MSHTA
- description: Detects Obfuscated Powershell via use MSHTA in Scripts
- category: data/rules/windows/builtin/system
- level: high
- id: 7e9c7999-0f9b-4d4a-a6ed-af6d553d4af4

Title: Hacktool Service Registration or Execution
- description: Detects PsExec service installation and execution events (service and Sysmon)
- category: data/rules/windows/builtin/system
- level: high
- id: d26ce60c-2151-403c-9a42-49420d87b5e4

Title: DHCP Server Error Failed Loading the CallOut DLL
- description: This rule detects a DHCP server error in which a specified Callout DLL (in registry) could not be loaded
- category: data/rules/windows/builtin/system
- level: critical
- id: 75edd3fd-7146-48e5-9848-3013d7f0282c

Title: Service Installation with Suspicious Folder Pattern
- description: Detects service installation with suspicious folder patterns
- category: data/rules/windows/builtin/system
- level: high
- id: 1b2ae822-6fe1-43ba-aa7c-d1a3b3d1d5f2

Title: CVE-2021-1675 Print Spooler Exploitation
- description: Detects driver load events print service operational log that are a sign of successful exploitation attempts ag
- category: data/rules/windows/builtin/printservice
- level: critical
- id: f34d942d-c8c4-4f1f-b196-22471aecf10a

Title: Possible CVE-2021-1675 Print Spooler Exploitation
- description: Detects events of driver load errors in print service logs that could be a sign of successful exploitation atte
- category: data/rules/windows/builtin/printservice
- level: high
- id: 4e64668a-4da1-49f5-a8df-9e2d5b866718

Title: File Was Not Allowed To Run
- description: Detect run not allowed files. Applocker is a very useful tool, especially on servers where unprivileged users h
- category: data/rules/windows/builtin/applocker
- level: medium
- id: 401e5d00-b944-11ea-8f9a-00163ecd60ae

Title: Code Integrity Blocked Driver Load
- description: Detects driver load events that got blocked by Windows code integrity checks
- category: data/rules/windows/builtin/code_integrity
- level: high
- id: f8931561-97f5-4c46-907f-0a4a592e47a7

Title: GALLIUM Artefacts
- description: Detects artefacts associated with activity group GALLIUM - Microsoft Threat Intelligence Center indicators rele
- category: data/rules/windows/builtin/dns_server
- level: high
- id: 3db10f25-2527-4b79-8d4b-471eb900ee29

Title: DNS Server Error Failed Loading the ServerLevelPluginDLL
- description: This rule detects a DNS server error in which a specified plugin DLL (in registry) could not be loaded
- category: data/rules/windows/builtin/dns_server
- level: critical
- id: cbe51394-cd93-4473-b555-edf0144952d9

Title: LDAP Reconnaissance / Active Directory Enumeration
- description: Detects possible Active Directory enumeration via LDAP
- category: data/rules/windows/builtin/ldap
- level: medium
- id: 31d68132-4038-47c7-8f8e-635a39a7c174

Title: Failed MSExchange Transport Agent Installation
- description: Detects a failed installation of a Exchange Transport Agent
- category: data/rules/windows/builtin/msexchange
- level: high
- id: c7d16cae-aaf3-42e5-9c1c-fb8553faa6fa

Title: Exchange Set OabVirtualDirectory ExternalUrl Property
- description: Rule to detect an adversary setting OabVirtualDirectory External URL property to a script in Exchange Managemen
- category: data/rules/windows/builtin/msexchange
- level: high
- id: 9db37458-4df2-46a5-95ab-307e7f29e675

Title: MSExchange Transport Agent Installation
- description: Detects the Installation of a Exchange Transport Agent
- category: data/rules/windows/builtin/msexchange
- level: medium
- id: 4fe151c2-ecf9-4fae-95ae-b88ec9c2fca6

Title: Certificate Request Export to Exchange Webserver
- description: Detects a write of an Exchange CSR to an untypical directory or with aspx name suffix which can be used to plac
- category: data/rules/windows/builtin/msexchange
- level: critical
- id: b7bc7038-638b-4ffd-880c-292c692209ef

Title: ProxyLogon MSExchange OabVirtualDirectory
- description: Detects specific patterns found after a successful ProxyLogon exploitation in relation to a Commandlet invocati
- category: data/rules/windows/builtin/msexchange
- level: critical
- id: 550d3350-bb8a-4ff3-9533-2ba533f4a1c0

Title: Possible Exploitation of Exchange RCE CVE-2021-42321
- description: Detects log entries that appear in exploitation attempts against MS Exchange RCE CVE-2021-42321
- category: data/rules/windows/builtin/msexchange
- level: critical
- id: c92f1896-d1d2-43c3-92d5-7a5b35c217bb

Title: Mailbox Export to Exchange Webserver
- description: Detects a successful export of an Exchange mailbox to untypical directory or with aspx name suffix which can be
- category: data/rules/windows/builtin/msexchange

- level: critical
- id: 516376b4-05cd-4122-bae0-ad7641c38d48

Title: Remove Exported Mailbox from Exchange Webserver
- description: Detects removal of an exported Exchange mailbox which could be to cover tracks from ProxyShell exploit
- category: data/rules/windows/builtin/msexchange
- level: high
- id: 09570ae5-889e-43ea-aac0-0e1221fb3d95

Title: HybridConnectionManager Service Running
- description: Rule to detect the Hybrid Connection Manager service running on an endpoint.
- category: data/rules/windows/builtin/servicebus
- level: high
- id: b55d23e5-6821-44ff-8a6e-67218891e49f

Title: Rare Scheduled Task Creations
- description: This rule detects rare scheduled task creations. Typically software gets installed on multiple systems and not
- category: data/rules/windows/builtin/taskscheduler
- level: low
- id: b20f6158-9438-41be-83da-a5a16ac90c2b

Title: Failed to Load Policy in Windows Firewall with Advanced Security
- description: The Windows Firewall service failed to load Group Policy.
- category: data/rules/windows/builtin/firewall_as
- level: low
- id: 7ec15688-fd24-4177-ba43-1a950537ee39

Title: Setting Change in Windows Firewall with Advanced Security
- description: Setting have been change in Windows Firewall
- category: data/rules/windows/builtin/firewall_as
- level: low
- id: 00bb5bd5-1379-4fcf-a965-a5b6f7478064

Title: Delete Rule in Windows Firewall with Advanced Security
- description: A rule has been deleted in the Windows Firewall exception list.
- category: data/rules/windows/builtin/firewall_as
- level: medium
- id: c187c075-bb3e-4c62-b4fa-beae0ffc211f

Title: Added Rule in Windows Firewall with Advanced Security
- description: A rule has been modified in the Windows Firewall exception list
- category: data/rules/windows/builtin/firewall_as
- level: medium
- id: cde0a575-7d3d-4a49-9817-b8004a7bf105

Title: Reset to Default Configuration Windows Firewall with Advanced Security
- description: Windows Firewall has been reset to its default configuration.
- category: data/rules/windows/builtin/firewall_as
- level: low
- id: 04b60639-39c0-412a-9fbe-e82499c881a3

Title: Modified Rule in Windows Firewall with Advanced Security
- description: A rule has been modified in the Windows Firewall exception list
- category: data/rules/windows/builtin/firewall_as
- level: low
- id: 5570c4d9-8fdd-4622-965b-403a5a101aa0

Title: Suspicious Task Added by Bitsadmin
- description: Adversaries may abuse BITS jobs to persistently execute or clean up after malicious payloads.

Windows Background Intelligent Transfer Service (BITS) is a low-bandwidth, asynchronous file transfer mechanism exposed through Component Object Model

- category: data/rules/windows/builtin/bits_client
- level: low
- id: 1ff315dc-2a3a-4b71-8dde-873818d25d39

Title: Suspicious Download File Extension with Bits
- description: Adversaries may abuse BITS jobs to persistently execute or clean up after malicious payloads.

Windows Background Intelligent Transfer Service (BITS) is a low-bandwidth, asynchronous file transfer mechanism exposed through Component Object Model

- category: data/rules/windows/builtin/bits_client
- level: low
- id: b85e5894-9b19-4d86-8c87-a2f3b81f0521

Title: Suspicious Task Added by Powershell
- description: Adversaries may abuse BITS jobs to persistently execute or clean up after malicious payloads.

Windows Background Intelligent Transfer Service (BITS) is a low-bandwidth, asynchronous file transfer mechanism exposed through Component Object Model

- category: data/rules/windows/builtin/bits_client
- level: low
- id: fe3a2d49-f255-4d10-935c-bda7391108eb

Title: Reconnaissance Activity
- description: Detects activity as "net user administrator /domain" and "net group domain admins /domain"
- category: data/rules/windows/builtin/security
- level: high
- id: 968eef52-9cff-4454-8992-1e74b9cbad6c

Title: DCERPC SMB Spoolss Named Pipe
- description: Detects the use of the spoolss named pipe over SMB. This can be used to trigger the authentication via NTLM of
- category: data/rules/windows/builtin/security
- level: medium
- id: 214e8f95-100a-4e04-bb31-ef6cba8ce07e

Title: Meterpreter or Cobalt Strike Getsystem Service Installation
- description: Detects the use of getsystem Meterpreter/Cobalt Strike command by detecting a specific service installation
- category: data/rules/windows/builtin/security
- level: critical
- id: ecbc5e16-58e0-4521-9c60-eb9a7ea4ad34

Title: VSSAudit Security Event Source Registration
- description: Detects the registration of the security event source VSSAudit. It would usually trigger when volume shadow cop
- category: data/rules/windows/builtin/security
- level: informational
- id: e9faba72-4974-4ab2-a4c5-46e25ad59e9b

Title: WCE wceaux.dll Access
- description: Detects wceaux.dll access while WCE pass-the-hash remote command execution on source host
- category: data/rules/windows/builtin/security
- level: critical
- id: 1de68c67-af5c-4097-9c85-fe5578e09e67

Title: Enabled User Right in AD to Control User Objects
- description: Detects scenario where if a user is assigned the SeEnableDelegationPrivilege right in Active Directory it would
- category: data/rules/windows/builtin/security
- level: high
- id: 311b6ce2-7890-4383-a8c2-663a9f6b43cd

Title: Powerview Add-DomainObjectAcl DCSync AD Extend Right
- description: backdooring domain object to grant the rights associated with DCSync to a regular user or machine account using
- category: data/rules/windows/builtin/security
- level: critical
- id: 2c99737c-585d-4431-b61a-c911d86ff32f

Title: Malicious Service Installations
- description: Detects known malicious service installs that only appear in cases of lateral movement, credential dumping, and
- category: data/rules/windows/builtin/security
- level: critical
- id: cb062102-587e-4414-8efa-dbe3c7bf19c6

Title: DPAPI Domain Backup Key Extraction
- description: Detects tools extracting LSA secret DPAPI domain backup key from Domain Controllers
- category: data/rules/windows/builtin/security
- level: critical
- id: 4ac1f50b-3bd0-4968-902d-868b4647937e

Title: ISO Image Mount
- description: Detects the mount of ISO images on an endpoint

- category: data/rules/windows/builtin/security
- level: medium
- id: 0248a7bc-8a9a-4cd8-a57e-3ae8e073a073

Title: KrbRelayUp Attack Pattern
- description: Detects logon events that have characteristics of events generated during an attack with KrbRelayUp and the lik
- category: data/rules/windows/builtin/security
- level: high
- id: 749c9f5e-b353-4b90-a9c1-05243357ca4b

Title: Persistence and Execution at Scale via GPO Scheduled Task
- description: Detect lateral movement using GPO scheduled task, usually used to deploy ransomware at scale
- category: data/rules/windows/builtin/security
- level: high
- id: a8f29a7b-b137-4446-80a0-b804272f3da2

Title: SAM Registry Hive Handle Request
- description: Detects handles requested to SAM registry hive
- category: data/rules/windows/builtin/security
- level: critical
- id: f8748f2c-89dc-4d95-afb0-5a2dfdbad332

Title: Correct Execution of Nltest.exe
- description: The attacker might use LOLBAS nltest.exe for discovery of domain controllers, domain trusts, parent domain and
- category: data/rules/windows/builtin/security
- level: high
- id: eeb66bbb-3dde-4582-815a-584aee9fe6d1

Title: T1047 Wmiprvse Wbemcomn DLL Hijack
- description: Detects a threat actor creating a file named `wbemcomn.dll` in the `C:\Windows\System32\wbem\` directory over t
- category: data/rules/windows/builtin/security
- level: critical
- id: f6c68d5f-e101-4b86-8c84-7d96851fd65c

Title: PowerShell Scripts Installed as Services
- description: Detects powershell script installed as a Service
- category: data/rules/windows/builtin/security
- level: high
- id: 2a926e6a-4b81-4011-8a96-e36cc8c04302

Title: Invoke-Obfuscation VAR+ Launcher
- description: Detects Obfuscated use of Environment Variables to execute PowerShell
- category: data/rules/windows/builtin/security
- level: high
- id: dcf2db1f-f091-425b-a821-c05875b8925a

Title: AD Object WriteDAC Access
- description: Detects WRITE_DAC access to a domain object
- category: data/rules/windows/builtin/security
- level: critical
- id: 028c7842-4243-41cd-be6f-12f3cf1a26c7

Title: Failed Logins with Different Accounts from Single Source System
- description: Detects suspicious failed logins with different user accounts from a single source system
- category: data/rules/windows/builtin/security
- level: medium
- id: 6309ffc4-8fa2-47cf-96b8-a2f72e58e538

Title: Interactive Logon to Server Systems
- description: Detects interactive console logons to Server Systems
- category: data/rules/windows/builtin/security
- level: medium
- id: 3ff152b2-1388-4984-9cd9-a323323fdadf

Title: Security Event Log Cleared
- description: Checks for event id 1102 which indicates the security event log was cleared.
- category: data/rules/windows/builtin/security
- level: medium
- id: a122ac13-daf8-4175-83a2-72c387be339d

Title: Suspicious PsExec Execution
- description: detects execution of psexec or paexec with renamed service name, this rule helps to filter out the noise if pse
- category: data/rules/windows/builtin/security
- level: high
- id: c462f537-a1e3-41a6-b5fc-b2c2cef9bf82

Title: Successful Overpass the Hash Attempt
- description: Detects successful logon with logon type 9 (NewCredentials) which matches the Overpass the Hash behavior of e.g
- category: data/rules/windows/builtin/security
- level: high
- id: 192a0330-c20b-4356-90b6-7b7049ae0b87

Title: Valid Users Failing to Authenticate From Single Source Using Kerberos
- description: Detects multiple failed logins with multiple valid domain accounts from a single source system using the Kerber
- category: data/rules/windows/builtin/security
- level: medium
- id: 5d1d946e-32e6-4d9a-a0dc-0ac022c7eb98

Title: Invoke-Obfuscation Via Stdin
- description: Detects Obfuscated Powershell via Stdin in Scripts
- category: data/rules/windows/builtin/security
- level: high
- id: 80b708f3-d034-40e4-a6c8-d23b7a7db3d1

Title: Invoke-Obfuscation Via Use Rundll32
- description: Detects Obfuscated Powershell via use Rundll32 in Scripts
- category: data/rules/windows/builtin/security
- level: high
- id: cd0f7229-d16f-42de-8fe3-fba365fbcb3a

Title: DPAPI Domain Master Key Backup Attempt
- description: Detects anyone attempting a backup for the DPAPI Master Key. This events gets generated at the source and not t
- category: data/rules/windows/builtin/security
- level: critical
- id: 39a94fd1-8c9a-4ff6-bf22-c058762f8014

Title: Sysmon Channel Reference Deletion
- description: Potential threat actor tampering with Sysmon manifest and eventually disabling it
- category: data/rules/windows/builtin/security
- level: critical
- id: 18beca67-ab3e-4ee3-ba7a-a46ca8d7d0cc

Title: Admin User Remote Logon
- description: Detect remote login by Administrator user (depending on internal pattern).
- category: data/rules/windows/builtin/security
- level: low
- id: 0f63e1ef-1eb9-4226-9d54-8927ca08520a

Title: Transferring Files with Credential Data via Network Shares
- description: Transferring files with well-known filenames (sensitive files with credential data) using network shares
- category: data/rules/windows/builtin/security
- level: medium
- id: 910ab938-668b-401b-b08c-b596e80fdca5

Title: Processes Accessing the Microphone and Webcam
- description: Potential adversaries accessing the microphone and webcam in an endpoint.
- category: data/rules/windows/builtin/security
- level: medium
- id: 8cd538a4-62d5-4e83-810b-12d41e428d6e

Title: AD Privileged Users or Groups Reconnaissance
- description: Detect priv users or groups recon based on 4661 eventid and known privileged users or groups SIDs
- category: data/rules/windows/builtin/security
- level: high
- id: 35ba1d85-724d-42a3-889f-2e2362bcaf23

Title: Multiple Users Attempting To Authenticate Using Explicit Credentials
- description: Detects a source user failing to authenticate with multiple users using explicit credentials on a host.

- category: data/rules/windows/builtin/security
- level: medium
- id: 196a29c2-e378-48d8-ba07-8a9e61f7fab9

Title: ADCS Certificate Template Configuration Vulnerability
- description: Detects certificate creation with template allowing risk permission subject
- category: data/rules/windows/builtin/security
- level: low
- id: 5ee3a654-372f-11ec-8d3d-0242ac130003

Title: CobaltStrike Service Installations
- description: Detects known malicious service installs that appear in cases in which a Cobalt Strike beacon elevates privileg
- category: data/rules/windows/builtin/security
- level: critical
- id: d7a95147-145f-4678-b85d-d1ff4a3bb3f6

Title: Remote Service Activity via SVCCTL Named Pipe
- description: Detects remote service activity via remote access to the svcctl named pipe
- category: data/rules/windows/builtin/security
- level: medium
- id: 586a8d6b-6bfe-4ad9-9d78-888cd2fe50c3

Title: Denied Access To Remote Desktop
- description: This event is generated when an authenticated user who is not allowed to log on remotely attempts to connect to
- category: data/rules/windows/builtin/security
- level: medium
- id: 8e5c03fa-b7f0-11ea-b242-07e0576828d9

Title: Mimikatz DC Sync
- description: Detects Mimikatz DC sync security events
- category: data/rules/windows/builtin/security
- level: high
- id: 611eab06-a145-4dfa-a295-3ccc5c20f59a

Title: Invoke-Obfuscation Obfuscated IEX Invocation
- description: Detects all variations of obfuscated powershell IEX invocation code generated by Invoke-Obfuscation framework f
- category: data/rules/windows/builtin/security
- level: high
- id: fd0f5778-d3cb-4c9a-9695-66759d04702a

Title: Scheduled Task Deletion
- description: Detects scheduled task deletion events. Scheduled tasks are likely to be deleted if not used for persistence. M
- category: data/rules/windows/builtin/security
- level: low
- id: 4f86b304-3e02-40e3-aa5d-e88a167c9617

Title: ADCS Certificate Template Configuration Vulnerability with Risky EKU
- description: Detects certificate creation with template allowing risk permission subject and risky EKU
- category: data/rules/windows/builtin/security
- level: high
- id: bfbd3291-de87-4b7c-88a2-d6a5deb28668

Title: Password Change on Directory Service Restore Mode (DSRM) Account
- description: The Directory Service Restore Mode (DSRM) account is a local administrator account on Domain Controllers. Attac
- category: data/rules/windows/builtin/security
- level: high
- id: 53ad8e36-f573-46bf-97e4-15ba5bf4bb51

Title: New or Renamed User Account with '$' in Attribute 'SamAccountName'
- description: Detects possible bypass EDR and SIEM via abnormal user account name.
- category: data/rules/windows/builtin/security
- level: high
- id: cfeed607-6aa4-4bbd-9627-b637deb723c8

Title: WMI Persistence
- description: Detects suspicious WMI event filter and command line event consumer based on WMI and Security Logs.
- category: data/rules/windows/builtin/security
- level: medium
- id: f033f3f3-fd24-4995-97d8-a3bb17550a88

Title: Account Tampering - Suspicious Failed Logon Reasons
- description: This method uses uncommon error codes on failed logons to determine suspicious activity and tampering with acco
- category: data/rules/windows/builtin/security
- level: high
- id: 9eb99343-d336-4020-a3cd-67f3819e68ee

Title: Possible PetitPotam Coerce Authentication Attempt
- description: Detect PetitPotam coerced authentication activity.
- category: data/rules/windows/builtin/security
- level: high
- id: 1ce8c8a3-2723-48ed-8246-906ac91061a6

Title: COMPlus_ETWEnabled Registry Modification
- description: Potential adversaries stopping ETW providers recording loaded .NET assemblies.
- category: data/rules/windows/builtin/security
- level: critical
- id: a4c90ea1-2634-4ca0-adbb-35eae169b6fc

Title: PetitPotam Suspicious Kerberos TGT Request
- description: Detect suspicious Kerberos TGT requests. Once an attacer obtains a computer certificate by abusing Active Direc
- category: data/rules/windows/builtin/security
- level: high
- id: 6a53d871-682d-40b6-83e0-b7c1a6c4e3a5

Title: Protected Storage Service Access
- description: Detects access to a protected_storage service over the network. Potential abuse of DPAPI to extract domain back
- category: data/rules/windows/builtin/security
- level: critical
- id: 45545954-4016-43c6-855e-eae8f1c369dc

Title: Active Directory Replication from Non Machine Account
- description: Detects potential abuse of Active Directory Replication Service (ADRS) from a non machine account to request cr
- category: data/rules/windows/builtin/security
- level: critical
- id: 17d619c1-e020-4347-957e-1d1207455c93

Title: SCM Database Handle Failure
- description: Detects non-system users failing to get a handle of the SCM database.
- category: data/rules/windows/builtin/security
- level: critical
- id: 13addce7-47b2-4ca0-a98f-1de964d1d669

Title: Multiple Users Failing to Authenticate from Single Process
- description: Detects failed logins with multiple accounts from a single process on the system.
- category: data/rules/windows/builtin/security
- level: medium
- id: fe563ab6-ded4-4916-b49f-a3a8445fe280

Title: Rare Schtasks Creations
- description: Detects rare scheduled tasks creations that only appear a few times per time frame and could reveal password du
- category: data/rules/windows/builtin/security
- level: low
- id: b0d77106-7bb0-41fe-bd94-d1752164d066

Title: Invoke-Obfuscation COMPRESS OBFUSCATION
- description: Detects Obfuscated Powershell via COMPRESS OBFUSCATION
- category: data/rules/windows/builtin/security
- level: medium
- id: 7a922f1b-2635-4d6c-91ef-af228b198ad3

Title: SysKey Registry Keys Access
- description: Detects handle requests and access operations to specific registry keys to calculate the SysKey
- category: data/rules/windows/builtin/security
- level: critical
- id: 9a4ff3b8-6187-4fd2-8e8b-e0eae1129495

Title: RottenPotato Like Attack Pattern
- description: Detects logon events that have characteristics of events generated during an attack with RottenPotato and the l

- category: data/rules/windows/builtin/security
- level: high
- id: 16f5d8ca-44bd-47c8-acbe-6fc95a16c12f

Title: Generic Password Dumper Activity on LSASS
- description: Detects process handle on LSASS process with certain access mask
- category: data/rules/windows/builtin/security
- level: high
- id: 4a1b6da0-d94f-4fc3-98fc-2d9cb9e5ee76

Title: Hacktool Ruler
- description: This events that are generated when using the hacktool Ruler by Sensepost
- category: data/rules/windows/builtin/security
- level: high
- id: 24549159-ac1b-479c-8175-d42aea947cae

Title: Hidden Local User Creation
- description: Detects the creation of a local hidden user account which should not happen for event ID 4720.
- category: data/rules/windows/builtin/security
- level: high
- id: 7b449a5e-1db5-4dd0-a2dc-4e3a67282538

Title: Active Directory User Backdoors
- description: Detects scenarios where one can control another users or computers account without having to use their credenti
- category: data/rules/windows/builtin/security
- level: high
- id: 300bac00-e041-4ee2-9c36-e262656a6ecc

Title: Valid Users Failing to Authenticate from Single Source Using NTLM
- description: Detects failed logins with multiple valid domain accounts from a single source system using the NTLM protocol.
- category: data/rules/windows/builtin/security
- level: medium
- id: f88bab7f-b1f4-41bb-bdb1-4b8af35b0470

Title: External Disk Drive Or USB Storage Device
- description: Detects external diskdrives or plugged in USB devices , EventID 6416 on windows 10 or later
- category: data/rules/windows/builtin/security
- level: low
- id: f69a87ea-955e-4fb4-adb2-bb9fd6685632

Title: Suspicious Kerberos RC4 Ticket Encryption
- description: Detects service ticket requests using RC4 encryption type
- category: data/rules/windows/builtin/security
- level: medium
- id: 496a0e47-0a33-4dca-b009-9e6ca3591f39

Title: SMB Create Remote File Admin Share
- description: Look for non-system accounts SMB accessing a file with write (0x2) access mask via administrative share (i.e C$
- category: data/rules/windows/builtin/security
- level: high
- id: b210394c-ba12-4f89-9117-44a2464b9511

Title: Suspicious Remote Logon with Explicit Credentials
- description: Detects suspicious processes logging on with explicit credentials
- category: data/rules/windows/builtin/security
- level: medium
- id: 941e5c45-cda7-4864-8cea-bbb7458d194a

Title: Addition of Domain Trusts
- description: Addition of domains is seldom and should be verified for legitimacy.
- category: data/rules/windows/builtin/security
- level: medium
- id: 0255a820-e564-4e40-af2b-6ac61160335c

Title: Failed Logins with Different Accounts from Single Source System
- description: Detects suspicious failed logins with different user accounts from a single source system
- category: data/rules/windows/builtin/security
- level: medium
- id: e98374a6-e2d9-4076-9b5c-11bdb2569995

Title: Invoke-Obfuscation Via Use MSHTA
- description: Detects Obfuscated Powershell via use MSHTA in Scripts
- category: data/rules/windows/builtin/security
- level: high
- id: 9b8d9203-4e0f-4cd9-bb06-4cc4ea6d0e9a

Title: Password Dumper Activity on LSASS
- description: Detects process handle on LSASS process with certain access mask and object type SAM_DOMAIN
- category: data/rules/windows/builtin/security
- level: high
- id: aa1697b7-d611-4f9a-9cb2-5125b4ccfd5c

Title: Windows Network Access Suspicious desktop.ini Action
- description: Detects unusual processes accessing desktop.ini remotely over network share, which can be leveraged to alter ho
- category: data/rules/windows/builtin/security
- level: medium
- id: 35bc7e28-ee6b-492f-ab04-da58fcf6402e

Title: Metasploit Or Impacket Service Installation Via SMB PsExec
- description: Detects usage of Metasploit SMB PsExec (exploit/windows/smb/psexec) and Impacket psexec.py by triggering on spe
- category: data/rules/windows/builtin/security
- level: high
- id: 6fb63b40-e02a-403e-9ffd-3bcc1d749442

Title: Password Protected ZIP File Opened (Email Attachment)
- description: Detects the extraction of password protected ZIP archives. See the filename variable for more details on which
- category: data/rules/windows/builtin/security
- level: high
- id: 571498c8-908e-40b4-910b-d2369159a3da

Title: First Time Seen Remote Named Pipe
- description: This detection excludes known namped pipes accessible remotely and notify on newly observed ones, may help to d
- category: data/rules/windows/builtin/security
- level: high
- id: 52d8b0c6-53d6-439a-9e41-52ad442ad9ad

Title: Addition of SID History to Active Directory Object
- description: An attacker can use the SID history attribute to gain additional privileges.
- category: data/rules/windows/builtin/security
- level: medium
- id: 2632954e-db1c-49cb-9936-67d1ef1d17d2

Title: Password Protected ZIP File Opened (Suspicious Filenames)
- description: Detects the extraction of password protected ZIP archives with suspicious file names. See the filename variable
- category: data/rules/windows/builtin/security
- level: high
- id: 54f0434b-726f-48a1-b2aa-067df14516e4

Title: Remote Registry Management Using Reg Utility
- description: Remote registry management using REG utility from non-admin workstation
- category: data/rules/windows/builtin/security
- level: medium
- id: 68fcba0d-73a5-475e-a915-e8b4c576827e

Title: CVE-2021-1675 Print Spooler Exploitation IPC Access
- description: Detects remote printer driver load from Detailed File Share in Security logs that are a sign of successful expl
- category: data/rules/windows/builtin/security
- level: critical
- id: 8fe1c584-ee61-444b-be21-e9054b229694

Title: NetNTLM Downgrade Attack
- description: Detects NetNTLM downgrade attack
- category: data/rules/windows/builtin/security
- level: critical
- id: d3abac66-f11c-4ed0-8acb-50cc29c97eed

Title: LSASS Access from Non System Account
- description: Detects potential mimikatz-like tools accessing LSASS from non system account

- category: data/rules/windows/builtin/security
- level: critical
- id: 962fe167-e48d-4fd6-9974-11e5b9a5d6d1

Title: Operation Wocao Activity
- description: Detects activity mentioned in Operation Wocao report
- category: data/rules/windows/builtin/security
- level: high
- id: 74ad4314-482e-4c3e-b237-3f7ed3b9ca8d

Title: Defrag Deactivation
- description: Detects the deactivation and disabling of the Scheduled defragmentation task as seen by Slingshot APT group
- category: data/rules/windows/builtin/security
- level: medium
- id: c5a178bf-9cfb-4340-b584-e4df39b6a3e7

Title: Metasploit SMB Authentication
- description: Alerts on Metasploit host's authentications on the domain.
- category: data/rules/windows/builtin/security
- level: high
- id: 72124974-a68b-4366-b990-d30e0b2a190d

Title: Invalid Users Failing To Authenticate From Source Using Kerberos
- description: Detects failed logins with multiple invalid domain accounts from a single source system using the Kerberos prot
- category: data/rules/windows/builtin/security
- level: medium
- id: bc93dfe6-8242-411e-a2dd-d16fa0cc8564

Title: Invoke-Obfuscation CLIP+ Launcher
- description: Detects Obfuscated use of Clip.exe to execute PowerShell
- category: data/rules/windows/builtin/security
- level: high
- id: 4edf51e1-cb83-4e1a-bc39-800e396068e3

Title: Multiple Users Remotely Failing To Authenticate From Single Source
- description: Detects a source system failing to authenticate against a remote host with multiple users.
- category: data/rules/windows/builtin/security
- level: medium
- id: add2ef8d-dc91-4002-9e7e-f2702369f53a

Title: Suspicious Access to Sensitive File Extensions
- description: Detects known sensitive file extensions accessed on a network share
- category: data/rules/windows/builtin/security
- level: medium
- id: 91c945bc-2ad1-4799-a591-4d00198a1215

Title: RDP Login from Localhost
- description: RDP login with localhost source address may be a tunnelled login
- category: data/rules/windows/builtin/security
- level: high
- id: 51e33403-2a37-4d66-a574-1fda1782cc31

Title: Unauthorized System Time Modification
- description: Detect scenarios where a potentially unauthorized application or user is modifying the system time.
- category: data/rules/windows/builtin/security
- level: medium
- id: faa031b5-21ed-4e02-8881-2591f98d82ed

Title: Enumeration via the Global Catalog
- description: Detects enumeration of the global catalog (that can be performed using BloodHound or others AD reconnaissance t
- category: data/rules/windows/builtin/security
- level: medium
- id: 619b020f-0fd7-4f23-87db-3f51ef837a34

Title: Local User Creation
- description: Detects local user creation on windows servers, which shouldn't happen in an Active Directory environment. Appl
- category: data/rules/windows/builtin/security
- level: low
- id: 66b6be3d-55d0-4f47-9855-d69df21740ea

Title: Windows Defender Exclusion Set
- description: Detects scenarios where an windows defender exclusion was added in registry where an entity would want to bypas
- category: data/rules/windows/builtin/security
- level: high
- id: e9c8808f-4cfb-4ba9-97d4-e5f3beaa244d

Title: Failed Code Integrity Checks
- description: Code integrity failures may indicate tampered executables.
- category: data/rules/windows/builtin/security
- level: low
- id: 470ec5fa-7b4e-4071-b200-4c753100f49b

Title: Invoke-Obfuscation VAR++ LAUNCHER OBFUSCATION
- description: Detects Obfuscated Powershell via VAR++ LAUNCHER
- category: data/rules/windows/builtin/security
- level: high
- id: 4c54ba8f-73d2-4d40-8890-d9cf1dca3d30

Title: Chafer Activity
- description: Detects Chafer activity attributed to OilRig as reported in Nyotron report in March 2018
- category: data/rules/windows/builtin/security
- level: critical
- id: c0580559-a6bd-4ef6-b9b7-83703d98b561

Title: Invoke-Obfuscation Via Use Clip
- description: Detects Obfuscated Powershell via use Clip.exe in Scripts
- category: data/rules/windows/builtin/security
- level: high
- id: 1a0a2ff1-611b-4dac-8216-8a7b47c618a6

Title: Possible Remote Password Change Through SAMR
- description: Detects a possible remote NTLM hash change through SAMR API SamiChangePasswordUser() or SamSetInformationUser()
- category: data/rules/windows/builtin/security
- level: medium
- id: 7818b381-5eb1-4641-bea5-ef9e4cfb5951

Title: Kerberos Manipulation
- description: This method triggers on rare Kerberos Failure Codes caused by manipulations of Kerberos messages
- category: data/rules/windows/builtin/security
- level: high
- id: f7644214-0eb0-4ace-9455-331ec4c09253

Title: Suspicious Driver Loaded By User
- description: Detects the loading of drivers via 'SeLoadDriverPrivilege' required to load or unload a device driver. With thi
- category: data/rules/windows/builtin/security
- level: medium
- id: f63508a0-c809-4435-b3be-ed819394d612

Title: Azure AD Health Monitoring Agent Registry Keys Access
- description: This detection uses Windows security events to detect suspicious access attempts to the registry key of Azure A

This detection requires an access control entry (ACE) on the system access control list (SACL) of the following securable object HKLM\SOFTWARE\Microsoft\Microsoft Online\Reporting\MonitoringAgent.

- category: data/rules/windows/builtin/security
- level: medium
- id: ff151c33-45fa-475d-af4f-c2f93571f4fe

Title: Disabling Windows Event Auditing
- description: Detects scenarios where system auditing (ie: windows event log auditing) is disabled. This may be used in a sce
- category: data/rules/windows/builtin/security
- level: high
- id: 69aeb277-f15f-4d2d-b32a-55e883609563

Title: RDP over Reverse SSH Tunnel WFP
- description: Detects svchost hosting RDP termsvcs communicating with the loopback address
- category: data/rules/windows/builtin/security
- level: high

- id: 5bed80b6-b3e8-428e-a3ae-d3c757589e41

Title: Pass the Hash Activity 2
- description: Detects the attack technique pass the hash which is used to move laterally inside the network
- category: data/rules/windows/builtin/security
- level: medium
- id: 8eef149c-bd26-49f2-9e5a-9b00e3af499b

Title: SCM Database Privileged Operation
- description: Detects non-system users performing privileged operation os the SCM database
- category: data/rules/windows/builtin/security
- level: critical
- id: dae8171c-5ec6-4396-b210-8466585b53e9

Title: Disabled Users Failing To Authenticate From Source Using Kerberos
- description: Detects failed logins with multiple disabled domain accounts from a single source system using the Kerberos pro
- category: data/rules/windows/builtin/security
- level: medium
- id: 4b6fe998-b69c-46d8-901b-13677c9fb663

Title: Pass the Hash Activity
- description: Detects the attack technique pass the hash which is used to move laterally inside the network
- category: data/rules/windows/builtin/security
- level: medium
- id: f8d98d6c-7a07-4d74-b064-dd4a3c244528

Title: Invalid Users Failing To Authenticate From Single Source Using NTLM
- description: Detects failed logins with multiple invalid domain accounts from a single source system using the NTLM protocol
- category: data/rules/windows/builtin/security
- level: medium
- id: 56d62ef8-3462-4890-9859-7b41e541f8d5

Title: Suspicious Multiple File Rename Or Delete Occurred
- description: Detects multiple file rename or delete events occurrence within a specified period of time by a same user (thes
- category: data/rules/windows/builtin/security
- level: medium
- id: 97919310-06a7-482c-9639-92b67ed63cf8

Title: Secure Deletion with SDelete
- description: Detects renaming of file while deletion with SDelete tool.
- category: data/rules/windows/builtin/security
- level: medium
- id: 39a80702-d7ca-4a83-b776-525b1f86a36d

Title: Invoke-Obfuscation RUNDLL LAUNCHER
- description: Detects Obfuscated Powershell via RUNDLL LAUNCHER
- category: data/rules/windows/builtin/security
- level: medium
- id: f241cf1b-3a6b-4e1a-b4f9-133c00dd95ca

Title: User Added to Local Administrators
- description: This rule triggers on user accounts that are added to the local Administrators group, which could be legitimate
- category: data/rules/windows/builtin/security
- level: medium
- id: c265cf08-3f99-46c1-8d59-328247057d57

Title: HybridConnectionManager Service Installation
- description: Rule to detect the Hybrid Connection Manager service installation.
- category: data/rules/windows/builtin/security
- level: high
- id: 0ee4d8a5-4e67-4faf-acfa-62a78457d1f2

Title: AD User Enumeration
- description: Detects access to a domain user from a non-machine account
- category: data/rules/windows/builtin/security
- level: medium
- id: ab6bffca-beff-4baa-af11-6733f296d57a

Title: Access to ADMIN$ Share

- description: Detects access to $ADMIN share
- category: data/rules/windows/builtin/security
- level: low
- id: 098d7118-55bc-4912-a836-dc6483a8d150

Title: Register new Logon Process by Rubeus
- description: Detects potential use of Rubeus via registered new trusted logon process
- category: data/rules/windows/builtin/security
- level: critical
- id: 12e6d621-194f-4f59-90cc-1959e21e69f7

Title: Scanner PoC for CVE-2019-0708 RDP RCE Vuln
- description: Detects the use of a scanner by zerosum0x0 that discovers targets vulnerable to CVE-2019-0708 RDP RCE aka Blue
- category: data/rules/windows/builtin/security
- level: critical
- id: 8400629e-79a9-4737-b387-5db940ab2367

Title: Impacket PsExec Execution
- description: Detects execution of Impacket's psexec.py.
- category: data/rules/windows/builtin/security
- level: high
- id: 32d56ea1-417f-44ff-822b-882873f5f43b

Title: Suspicious Windows ANONYMOUS LOGON Local Account Created
- description: Detects the creation of suspicious accounts similar to ANONYMOUS LOGON, such as using additional spaces. Create
- category: data/rules/windows/builtin/security
- level: high
- id: 1bbf25b9-8038-4154-a50b-118f2a32be27

Title: Failed Logon From Public IP
- description: A login from a public IP can indicate a misconfigured firewall or network boundary.
- category: data/rules/windows/builtin/security
- level: medium
- id: f88e112a-21aa-44bd-9b01-6ee2a2bbbed1

Title: Suspicious Computer Account Name Change CVE-2021-42287
- description: Detects the renaming of an existing computer account to a account name that doesn't contain a $ symbol as seen
- category: data/rules/windows/builtin/security
- level: critical
- id: 45eb2ae2-9aa2-4c3a-99a5-6e5077655466

Title: T1021 DCOM InternetExplorer.Application Iertutil DLL Hijack
- description: Detects a threat actor creating a file named `iertutil.dll` in the `C:\Program Files\Internet Explorer\` direct
- category: data/rules/windows/builtin/security
- level: critical
- id: c39f0c81-7348-4965-ab27-2fde35a1b641

Title: Weak Encryption Enabled and Kerberoast
- description: Detects scenario where weak encryption is enabled for a user profile which could be used for hash/password crac
- category: data/rules/windows/builtin/security
- level: high
- id: f6de9536-0441-4b3f-a646-f4e00f300ffd

Title: Security Eventlog Cleared
- description: One of the Windows Eventlogs has been cleared. e.g. caused by "wevtutil cl" command execution
- category: data/rules/windows/builtin/security
- level: high
- id: d99b79d2-0a6f-4f46-ad8b-260b6e17f982

Title: Password Protected ZIP File Opened
- description: Detects the extraction of password protected ZIP archives. See the filename variable for more details on which
- category: data/rules/windows/builtin/security
- level: medium
- id: 00ba9da1-b510-4f6b-b258-8d338836180f

Title: Tap Driver Installation
- description: Well-known TAP software installation. Possible preparation for data exfiltration using tunnelling techniques
- category: data/rules/windows/builtin/security
- level: medium

- id: 9c8afa4d-0022-48f0-9456-3712466f9701

Title: Azure AD Health Service Agents Registry Keys Access
- description: This detection uses Windows security events to detect suspicious access attempts to the registry key values and

Information from AD Health service agents can be used to potentially abuse some of the features provided by those services in the cloud (e.g. Federation). This detection requires an access control entry (ACE) on the system access control list (SACL) of the following securable object: HKLM:\SOFTWARE\Microsoft\ADHealthAgent. Make sure you set the SACL to propagate to its sub-keys.

- category: data/rules/windows/builtin/security
- level: medium
- id: 1d2ab8ac-1a01-423b-9c39-001510eae8e8

Title: Login with WMI
- description: Detection of logins performed with WMI
- category: data/rules/windows/builtin/security
- level: low
- id: 5af54681-df95-4c26-854f-2565e13cfab0

Title: Remote Task Creation via ATSVC Named Pipe
- description: Detects remote task creation via at.exe or API interacting with ATSVC namedpipe
- category: data/rules/windows/builtin/security
- level: medium
- id: f6de6525-4509-495a-8a82-1f8b0ed73a00

Title: Suspicious Outbound Kerberos Connection
- description: Detects suspicious outbound network activity via kerberos default port indicating possible lateral movement or
- category: data/rules/windows/builtin/security
- level: high
- id: eca91c7c-9214-47b9-b4c5-cb1d7e4f2350

Title: Invoke-Obfuscation STDIN+ Launcher
- description: Detects Obfuscated use of stdin to execute PowerShell
- category: data/rules/windows/builtin/security
- level: high
- id: 0c718a5e-4284-4fb9-b4d9-b9a50b3a1974

Title: Remote PowerShell Sessions Network Connections (WinRM)
- description: Detects basic PowerShell Remoting (WinRM) by monitoring for network inbound connections to ports 5985 OR 5986
- category: data/rules/windows/builtin/security
- level: high
- id: 13acf386-b8c6-4fe0-9a6e-c4756b974698

Title: Possible Zerologon (CVE-2020-1472) Exploitation
- description: Detects Netlogon Elevation of Privilege Vulnerability aka Zerologon (CVE-2020-1472)
- category: data/rules/windows/builtin/security
- level: high
- id: dd7876d8-0f09-11eb-adc1-0242ac120002

Title: Possible Impacket SecretDump Remote Activity
- description: Detect AD credential dumping using impacket secretdump HKTL
- category: data/rules/windows/builtin/security
- level: high
- id: 252902e3-5830-4cf6-bf21-c22083dfd5cf

Title: Credential Dumping Tools Service Execution
- description: Detects well-known credential dumping tools execution via service execution events
- category: data/rules/windows/builtin/security
- level: high
- id: f0d1feba-4344-4ca9-8121-a6c97bd6df52

Title: Remote WMI ActiveScriptEventConsumers
- description: Detect potential adversaries leveraging WMI ActiveScriptEventConsumers remotely to move laterally in a network
- category: data/rules/windows/builtin/security
- level: high
- id: 9599c180-e3a8-4743-8f92-7fb96d3be648

Title: User Couldn't Call a Privileged Service 'LsaRegisterLogonProcess'
- description: The 'LsaRegisterLogonProcess' function verifies that the application making the function call is a logon proces

- category: data/rules/windows/builtin/security
- level: high
- id: 6daac7fc-77d1-449a-a71a-e6b4d59a0e54

Title: Possible DC Shadow
- description: Detects DCShadow via create new SPN
- category: data/rules/windows/builtin/security
- level: high
- id: 32e19d25-4aed-4860-a55a-be99cb0bf7ed

Title: Suspicious LDAP-Attributes Used
- description: Detects the usage of particular AttributeLDAPDisplayNames, which are known for data exchange via LDAP by the to
- category: data/rules/windows/builtin/security
- level: high
- id: d00a9a72-2c09-4459-ad03-5e0a23351e36

Title: An Application Is Uninstall
- description: An application have been remove check if it is a critical
- category: data/rules/windows/builtin/application
- level: low
- id: 570ae5ec-33dc-427c-b815-db86228ad43e

Title: Microsoft Malware Protection Engine Crash
- description: This rule detects a suspicious crash of the Microsoft Malware Protection Engine
- category: data/rules/windows/builtin/application
- level: high
- id: 6c82cf5c-090d-4d57-9188-533577631108

Title: Atera Agent Installation
- description: Detects successful installation of Atera Remote Monitoring & Management (RMM) agent as recently found to be use
- category: data/rules/windows/builtin/application
- level: high
- id: 87261fb2-69d0-42fe-b9de-88c6b5f65a43

Title: LPE InstallerFileTakeOver PoC CVE-2021-41379
- description: Detects PoC tool used to exploit LPE vulnerability CVE-2021-41379
- category: data/rules/windows/builtin/application
- level: high
- id: 7dbb86de-a0cc-494c-8aa8-b2996c9ef3c8

Title: Relevant Anti-Virus Event
- description: This detection method points out highly relevant Antivirus events
- category: data/rules/windows/builtin/application
- level: high
- id: 78bc5783-81d9-4d73-ac97-59f6db4f72a8

Title: Audit CVE Event
- description: Detects events generated by Windows to indicate the exploitation of a known vulnerability (e.g. CVE-2020-0601)
- category: data/rules/windows/builtin/application
- level: critical
- id: 48d91a3a-2363-43ba-a456-ca71ac3da5c2

Title: Backup Catalog Deleted
- description: Detects backup catalog deletions
- category: data/rules/windows/builtin/application
- level: medium
- id: 9703792d-fd9a-456d-a672-ff92efe4806a

Title: CVE-2020-0688 Exploitation via Eventlog
- description: Detects the exploitation of Microsoft Exchange vulnerability as described in CVE-2020-0688
- category: data/rules/windows/builtin/application
- level: high
- id: d6266bf5-935e-4661-b477-78772735a7cb

Title: Potential Remote Desktop Connection to Non-Domain Host
- description: Detects logons using NTLM to hosts that are potentially not part of the domain.
- category: data/rules/windows/builtin/ntlm
- level: medium
- id: ce5678bb-b9aa-4fb5-be4b-e57f686256ad

Title: NTLM Logon
- description: Detects logons using NTLM, which could be caused by a legacy source or attackers
- category: data/rules/windows/builtin/ntlm
- level: low
- id: 98c3bcf1-56f2-49dc-9d8d-c66cf190238b

Title: NTLM Brute Force
- description: Detects common NTLM brute force device names
- category: data/rules/windows/builtin/ntlm
- level: medium
- id: 9c8acf1a-cbf9-4db6-b63c-74baabe03e59

Title: USB Device Plugged
- description: Detects plugged USB devices
- category: data/rules/windows/builtin/driverframeworks
- level: low
- id: 1a4bd6e3-4c6e-405d-a9a3-53a116e341d4

Title: LSASS Access Detected via Attack Surface Reduction
- description: Detects Access to LSASS Process
- category: data/rules/windows/builtin/windefend
- level: high
- id: a0a278fe-2c0e-4de2-ac3c-c68b08a9ba98

Title: PSExec and WMI Process Creations Block
- description: Detects blocking of process creations originating from PSExec and WMI commands
- category: data/rules/windows/builtin/windefend
- level: high
- id: 97b9ce1e-c5ab-11ea-87d0-0242ac130003

Title: Windows Defender Threat Detection Disabled
- description: Detects disabling Windows Defender threat protection
- category: data/rules/windows/builtin/windefend
- level: low
- id: fe34868f-6e0e-4882-81f6-c43aa8f15b62

Title: Windows Defender Exclusions Added
- description: Detects the Setting of Windows Defender Exclusions
- category: data/rules/windows/builtin/windefend
- level: medium
- id: 1321dc4e-a1fe-481d-a016-52c45f0c8b4f

Title: Microsoft Defender Tamper Protection Trigger
- description: Detects block of attempt to disable real time protection of Microsoft Defender by tamper protection
- category: data/rules/windows/builtin/windefend
- level: critical
- id: 49e5bc24-8b86-49f1-b743-535f332c2856

Title: Windows Defender AMSI Trigger Detected
- description: Detects triggering of AMSI by Windows Defender.
- category: data/rules/windows/builtin/windefend
- level: high
- id: ea9bf0fa-edec-4fb8-8b78-b119f2528186

Title: Windows Defender Threat Detected
- description: Detects all actions taken by Windows Defender malware detection engines
- category: data/rules/windows/builtin/windefend
- level: high
- id: 57b649ef-ff42-4fb0-8bf6-62da243a1708

Title: Windows Defender Malware Detection History Deletion
- description: Windows Defender logs when the history of detected infections is deleted. Log file will contain the message "Wi
- category: data/rules/windows/builtin/windefend
- level: high
- id: 2afe6582-e149-11ea-87d0-0242ac130003

Title: Ngrok Usage with Remote Desktop Service
- description: Detects cases in which ngrok, a reverse proxy tool, forwards events to the local RDP port, which could be a sig

- category: data/rules/windows/builtin/terminalservices
- level: high
- id: 64d51a51-32a6-49f0-9f3d-17e34d640272

Title: WMI Persistence
- description: Detects suspicious WMI event filter and command line event consumer based on WMI and Security Logs.
- category: data/rules/windows/builtin/wmi
- level: medium
- id: 0b7889b4-5577-4521-a60a-3376ee7f9f7b

Title: Suspicious Rejected SMB Guest Logon From IP
- description: Detect Attempt PrintNightmare (CVE-2021-1675) Remote code execution in Windows Spooler Service
- category: data/rules/windows/builtin/smbclient
- level: medium
- id: 71886b70-d7b4-4dbf-acce-87d2ca135262

Title: PowerShell Network Connections
- description: Detects a Powershell process that opens network connections - check for suspicious target ports and target syst
- category: data/rules/windows/network_connection
- level: low
- id: 1f21ec3f-810d-4b0e-8045-322202e22b4b

Title: Suspicious Outbound RDP Connections
- description: Detects Non-Standard Tools Connecting to TCP port 3389 indicating possible lateral movement
- category: data/rules/windows/network_connection
- level: high
- id: ed74fe75-7594-4b4b-ae38-e38e3fd2eb23

Title: Microsoft Binary Suspicious Communication Endpoint
- description: Detects an executable in the Windows folder accessing suspicious domains
- category: data/rules/windows/network_connection
- level: high
- id: e0f8ab85-0ac9-423b-a73a-81b3c7b1aa97

Title: Download a File with IMEWDBLD.exe
- description: Use IMEWDBLD.exe (built-in to windows) to download a file
- category: data/rules/windows/network_connection
- level: high
- id: 8d7e392e-9b28-49e1-831d-5949c6281228

Title: Communication To Mega.nz
- description: Detects an executable accessing mega.co.nz, which could be a sign of forbidden file sharing use of data exfiltr
- category: data/rules/windows/network_connection
- level: high
- id: fdeebdf0-9f3f-4d08-84a6-4c4d13e39fe4

Title: Rundll32 Internet Connection
- description: Detects a rundll32 that communicates with public IP addresses
- category: data/rules/windows/network_connection
- level: medium
- id: cdc8da7d-c303-42f8-b08c-b4ab47230263

Title: Notepad Making Network Connection
- description: Detects suspicious network connection by Notepad
- category: data/rules/windows/network_connection
- level: high
- id: e81528db-fc02-45e8-8e98-4e84aba1f10b

Title: Suspicious Program Location with Network Connections
- description: Detects programs with network connections running in suspicious files system locations
- category: data/rules/windows/network_connection
- level: high
- id: 7b434893-c57d-4f41-908d-6a17bf1ae98f

Title: Windows Crypto Mining Pool Connections
- description: Detects process connections to a Monero crypto mining pool
- category: data/rules/windows/network_connection
- level: high
- id: fa5b1358-b040-4403-9868-15f7d9ab6329

Title: RDP Over Reverse SSH Tunnel
- description: Detects svchost hosting RDP termsvcs communicating with the loopback address and on TCP port 3389
- category: data/rules/windows/network_connection
- level: high
- id: 5f699bc5-5446-4a4a-a0b7-5ef2885a3eb4

Title: Suspicious Dropbox API Usage
- description: Detects an executable that isn't dropbox but communicates with the Dropbox API
- category: data/rules/windows/network_connection
- level: high
- id: 25eabf56-22f0-4915-a1ed-056b8dae0a68

Title: Wuauclt Network Connection
- description: Detects the use of the Windows Update Client binary (wuauclt.exe) to proxy execute code and making a network co
- category: data/rules/windows/network_connection
- level: medium
- id: c649a6c7-cd8c-4a78-9c04-000fc76df954

Title: Microsoft Binary Github Communication
- description: Detects an executable in the Windows folder accessing github.com
- category: data/rules/windows/network_connection
- level: high
- id: 635dbb88-67b3-4b41-9ea5-a3af2dd88153

Title: Excel Network Connections
- description: Detects an Excel process that opens suspicious network connections to non-private IP addresses, and attempts to
- category: data/rules/windows/network_connection
- level: medium
- id: 75e33ce3-ae32-4dcc-9aa8-a2a3029d6f84

Title: Silenttrinity Stager Msbuild Activity
- description: Detects a possible remote connections to Silenttrinity c2
- category: data/rules/windows/network_connection
- level: high
- id: 50e54b8d-ad73-43f8-96a1-5191685b17a4

Title: RDP to HTTP or HTTPS Target Ports
- description: Detects svchost hosting RDP termsvcs communicating to target systems on TCP port 80 or 443
- category: data/rules/windows/network_connection
- level: high
- id: b1e5da3b-ca8e-4adf-915c-9921f3d85481

Title: Suspicious Outbound Kerberos Connection
- description: Detects suspicious outbound network activity via kerberos default port indicating possible lateral movement or
- category: data/rules/windows/network_connection
- level: high
- id: e54979bd-c5f9-4d6c-967b-a04b19ac4c74

Title: Equation Editor Network Connection
- description: Detects network connections from Equation Editor
- category: data/rules/windows/network_connection
- level: high
- id: a66bc059-c370-472c-a0d7-f8fd1bf9d583

Title: Python Initiated Connection
- description: Adversaries may attempt to get a listing of services running on remote hosts, including those that may be vulne
- category: data/rules/windows/network_connection
- level: high
- id: bef0bc5a-b9ae-425d-85c6-7b2d705980c6

Title: Msiexec Initiated Connection
- description: Adversaries may abuse msiexec.exe to proxy execution of malicious payloads.

Msiexec.exe is the command-line utility for the Windows Installer and is thus commonly associated with executing installation packages (.msi)

- category: data/rules/windows/network_connection
- level: medium
- id: 8e5e38e4-5350-4c0b-895a-e872ce0dd54f

Title: Microsoft Sync Center Suspicious Network Connections
- description: Detects suspicious connections from Microsoft Sync Center to non-private IPs.
- category: data/rules/windows/network_connection
- level: medium
- id: 9f2cc74d-78af-4eb2-bb64-9cd1d292b87b

Title: Regsvr32 Network Activity
- description: Detects network connections and DNS queries initiated by Regsvr32.exe
- category: data/rules/windows/network_connection
- level: high
- id: c7e91a02-d771-4a6d-a700-42587e0b1095

Title: Suspicious Outbound SMTP Connections
- description: Adversaries may steal data by exfiltrating it over an un-encrypted network protocol other than that of the exis

The data may also be sent to an alternate network location from the main command and control server.

- category: data/rules/windows/network_connection
- level: medium
- id: 9976fa64-2804-423c-8a5b-646ade840773

Title: Suspicious Typical Malware Back Connect Ports
- description: Detects programs that connect to typical malware back connect ports based on statistical analysis from two diff
- category: data/rules/windows/network_connection
- level: medium
- id: 4b89abaa-99fe-4232-afdd-8f9aa4d20382

Title: Dllhost Internet Connection
- description: Detects Dllhost that communicates with public IP addresses
- category: data/rules/windows/network_connection
- level: medium
- id: cfed2f44-16df-4bf3-833a-79405198b277

Title: Remote PowerShell Session
- description: Detects remote PowerShell connections by monitoring network outbound connections to ports 5985 or 5986 from a n
- category: data/rules/windows/network_connection
- level: high
- id: c539afac-c12a-46ed-b1bd-5a5567c9f045

Title: Unsigned Image Loaded Into LSASS Process
- description: Loading unsigned image (DLL, EXE) into LSASS process
- category: data/rules/windows/image_load
- level: medium
- id: 857c8db3-c89b-42fb-882b-f681c7cf4da2

Title: UIPromptForCredentials DLLs
- description: Detects potential use of UIPromptForCredentials functions by looking for some of the DLLs needed for it.
- category: data/rules/windows/image_load
- level: medium
- id: 9ae01559-cf7e-4f8e-8e14-4c290a1b4784

Title: Suspicious Load of Advapi31.dll
- description: Detects the load of advapi31.dll by a process running in an uncommon folder
- category: data/rules/windows/image_load
- level: informational
- id: d813d662-785b-42ca-8b4a-f7457d78d5a9

Title: WMI Script Host Process Image Loaded
- description: Detects signs of the WMI script host process %SystemRoot%\system32\wbem\scrcons.exe functionality being used vi
- category: data/rules/windows/image_load
- level: high
- id: b439f47d-ef52-4b29-9a2f-57d8a96cb6b8

Title: Suspicious WSMAN Provider Image Loads
- description: Detects signs of potential use of the WSMAN provider from uncommon processes locally and remote execution.
- category: data/rules/windows/image_load
- level: medium
- id: ad1f4bb9-8dfb-4765-adb6-2a7cfb6c0f94

Title: Fax Service DLL Search Order Hijack
- description: The Fax service attempts to load ualapi.dll, which is non-existent. An attacker can then (side)load their own m
- category: data/rules/windows/image_load
- level: high
- id: 828af599-4c53-4ed2-ba4a-a9f835c434ea

Title: WMI Persistence - Command Line Event Consumer
- description: Detects WMI command line event consumers
- category: data/rules/windows/image_load
- level: high
- id: 05936ce2-ee05-4dae-9d03-9a391cf2d2c6

Title: CLR DLL Loaded Via Office Applications
- description: Detects CLR DLL being loaded by an Office Product
- category: data/rules/windows/image_load
- level: high
- id: d13c43f0-f66b-4279-8b2c-5912077c1780

Title: Suspicious System.Drawing Load
- description: A General detection for processes loading System.Drawing.ni.dll. This could be an indicator of potential Screen
- category: data/rules/windows/image_load
- level: low
- id: 666ecfc7-229d-42b8-821e-1a8f8cb7057c

Title: CLR DLL Loaded Via Scripting Applications
- description: Detects CLR DLL being loaded by an scripting applications
- category: data/rules/windows/image_load
- level: high
- id: 4508a70e-97ef-4300-b62b-ff27992990ea

Title: APT PRIVATELOG Image Load Pattern
- description: Detects an image load pattern as seen when a tool named PRIVATELOG is used and rarely observed under legitimate
- category: data/rules/windows/image_load
- level: high
- id: 33a2d1dd-f3b0-40bd-8baf-7974468927cc

Title: Pingback Backdoor
- description: Detects the use of Pingback backdoor that creates ICMP tunnel for C2 as described in the trustwave report
- category: data/rules/windows/image_load
- level: high
- id: 35a7dc42-bc6f-46e0-9f83-81f8e56c8d4b

Title: Abusing Azure Browser SSO
- description: Detects abusing Azure Browser SSO by requesting OAuth 2.0 refresh tokens for an Azure-AD-authenticated Windows
- category: data/rules/windows/image_load
- level: high
- id: 50f852e6-af22-4c78-9ede-42ef36aa3453

Title: Active Directory Kerberos DLL Loaded Via Office Applications
- description: Detects Kerberos DLL being loaded by an Office Product
- category: data/rules/windows/image_load
- level: high
- id: 7417e29e-c2e7-4cf6-a2e8-767228c64837

Title: Time Travel Debugging Utility Usage
- description: Detects usage of Time Travel Debugging Utility. Adversaries can execute malicious processes and dump processes,
- category: data/rules/windows/image_load
- level: high
- id: e76c8240-d68f-4773-8880-5c6f63595aaf

Title: Wmiprvse Wbemcomn DLL Hijack
- description: Detects a threat actor creating a file named `wbemcomn.dll` in the `C:\Windows\System32\wbem\` directory over t
- category: data/rules/windows/image_load
- level: critical
- id: 7707a579-e0d8-4886-a853-ce47e4575aaa

Title: Load of dbghelp/dbgcore DLL from Suspicious Process
- description: Detects the load of dbghelp/dbgcore DLL (used to make memory dumps) by suspicious processes. Tools like Process

- category: data/rules/windows/image_load
- level: high
- id: 0e277796-5f23-4e49-a490-483131d4f6e1

Title: Image Load of VSS_PS.dll by Uncommon Executable
- description: Detects the image load of vss_ps.dll by uncommon executables using OriginalFileName datapoint
- category: data/rules/windows/image_load
- level: high
- id: 333cdbe8-27bb-4246-bf82-b41a0dca4b70

Title: SILENTTRINITY Stager Execution
- description: Detects SILENTTRINITY stager use
- category: data/rules/windows/image_load
- level: high
- id: 75c505b1-711d-4f68-a357-8c3fe37dbf2d

Title: GAC DLL Loaded Via Office Applications
- description: Detects any GAC DLL being loaded by an Office Product
- category: data/rules/windows/image_load
- level: high
- id: 90217a70-13fc-48e4-b3db-0d836c5824ac

Title: Windows Spooler Service Suspicious Binary Load
- description: Detect DLL Load from Spooler Service backup folder
- category: data/rules/windows/image_load
- level: informational
- id: 02fb90de-c321-4e63-a6b9-25f4b03dfd14

Title: In-memory PowerShell
- description: Detects loading of essential DLL used by PowerShell, but not by the process powershell.exe. Detects meterpreter
- category: data/rules/windows/image_load
- level: medium
- id: 092bc4b9-3d1d-43b4-a6b4-8c8acd83522f

Title: Alternate PowerShell Hosts
- description: Detects alternate PowerShell hosts potentially bypassing detections looking for powershell.exe
- category: data/rules/windows/image_load
- level: medium
- id: fe6e002f-f244-4278-9263-20e4b593827f

Title: PCRE.NET Package Image Load
- description: Detects processes loading modules related to PCRE.NET package
- category: data/rules/windows/image_load
- level: high
- id: 84b0a8f3-680b-4096-a45b-e9a89221727c

Title: Mimikatz In-Memory
- description: Detects certain DLL loads when Mimikatz gets executed
- category: data/rules/windows/image_load
- level: medium
- id: c0478ead-5336-46c2-bd5e-b4c84bc3a36e

Title: Python Py2Exe Image Load
- description: Detects the image load of Python Core indicative of a Python script bundled with Py2Exe.
- category: data/rules/windows/image_load
- level: medium
- id: cbb56d62-4060-40f7-9466-d8aaf3123f83

Title: FoggyWeb Backdoor DLL Loading
- description: Detects DLL image load activity as used by FoggyWeb backdoor loader
- category: data/rules/windows/image_load
- level: critical
- id: 640dc51c-7713-4faa-8a0e-e7c0d9d4654c

Title: dotNET DLL Loaded Via Office Applications
- description: Detects any assembly DLL being loaded by an Office Product
- category: data/rules/windows/image_load
- level: high
- id: ff0f2b05-09db-4095-b96d-1b75ca24894a

Title: UAC Bypass With Fake DLL
- description: Attempts to load dismcore.dll after dropping it
- category: data/rules/windows/image_load
- level: high
- id: a5ea83a7-05a5-44c1-be2e-addccbbd8c03

Title: WMI Modules Loaded
- description: Detects non wmiprvse loading WMI modules
- category: data/rules/windows/image_load
- level: informational
- id: 671bb7e3-a020-4824-a00e-2ee5b55f385e

Title: VBA DLL Loaded Via Microsoft Word
- description: Detects DLL's Loaded Via Word Containing VBA Macros
- category: data/rules/windows/image_load
- level: high
- id: e6ce8457-68b1-485b-9bdd-3c2b5d679aa9

Title: Active Directory Parsing DLL Loaded Via Office Applications
- description: Detects DSParse DLL being loaded by an Office Product
- category: data/rules/windows/image_load
- level: high
- id: a2a3b925-7bb0-433b-b508-db9003263cc4

Title: Svchost DLL Search Order Hijack
- description: IKEEXT and SessionEnv service, as they call LoadLibrary on files that do not exist within C:\Windows\System32\
- category: data/rules/windows/image_load
- level: high
- id: 602a1f13-c640-4d73-b053-be9a2fa58b77

Title: Possible Process Hollowing Image Loading
- description: Detects Loading of samlib.dll, WinSCard.dll from untypical process e.g. through process hollowing by Mimikatz
- category: data/rules/windows/image_load
- level: high
- id: e32ce4f5-46c6-4c47-ba69-5de3c9193cd7

Title: WMIC Loading Scripting Libraries
- description: Detects threat actors proxy executing code and bypassing application controls by leveraging wmic and the `/FORM
- category: data/rules/windows/image_load
- level: high
- id: 06ce37c2-61ab-4f05-9ff5-b1a96d18ae32

Title: ADFS Database Named Pipe Connection
- description: Detects suspicious local connections via a named pipe to the AD FS configuration database (Windows Internal Dat
- category: data/rules/windows/pipe_created
- level: high
- id: 1ea13e8c-03ea-409b-877d-ce5c3d2c1cb3

Title: Turla Group Named Pipes
- description: Detects a named pipe used by Turla group samples
- category: data/rules/windows/pipe_created
- level: critical
- id: 739915e4-1e70-4778-8b8a-17db02f66db1

Title: EfsPotato Named Pipe
- description: Detects the pattern of a pipe name as used by the tool EfsPotato
- category: data/rules/windows/pipe_created
- level: critical
- id: 637f689e-b4a5-4a86-be0e-0100a0a33ba2

Title: Malicious Named Pipe
- description: Detects the creation of a named pipe used by known APT malware
- category: data/rules/windows/pipe_created
- level: critical
- id: fe3ac066-98bb-432a-b1e7-a5229cb39d4a

Title: WMI Event Consumer Created Named Pipe
- description: Detects the WMI Event Consumer service scrcons.exe creating a named pipe

- category: data/rules/windows/pipe_created
- level: high
- id: 493fb4ab-cdcc-4c4f-818c-0e363bd1e4bb

Title: T1086 PowerShell Execution
- description: Detects execution of PowerShell
- category: data/rules/windows/pipe_created
- level: informational
- id: ac7102b4-9e1e-4802-9b4f-17c5524c015c

Title: Alternate PowerShell Hosts Pipe
- description: Detects alternate PowerShell hosts potentially bypassing detections looking for powershell.exe
- category: data/rules/windows/pipe_created
- level: medium
- id: 58cb02d5-78ce-4692-b3e1-dce850aae41a

Title: CobaltStrike Named Pipe Patterns
- description: Detects the creation of a named pipe with a pattern found in CobaltStrike malleable C2 profiles
- category: data/rules/windows/pipe_created
- level: high
- id: 85adeb13-4fc9-4e68-8a4a-c7cb2c336eb7

Title: Cred Dump-Tools Named Pipes
- description: Detects well-known credential dumping tools execution via specific named pipes
- category: data/rules/windows/pipe_created
- level: critical
- id: 961d0ba2-3eea-4303-a930-2cf78bbfcc5e

Title: PsExec Pipes Artifacts
- description: Detecting use PsExec via Pipe Creation/Access to pipes
- category: data/rules/windows/pipe_created
- level: medium
- id: 9e77ed63-2ecf-4c7b-b09d-640834882028

Title: PsExec Tool Execution
- description: Detects PsExec service installation and execution events (service and Sysmon)
- category: data/rules/windows/pipe_created
- level: low
- id: f3f3a972-f982-40ad-b63c-bca6afdfad7c

Title: CobaltStrike Named Pipe Pattern Regex
- description: Detects the creation of a named pipe matching a pattern used by CobaltStrike Malleable C2 profiles
- category: data/rules/windows/pipe_created
- level: critical
- id: 0e7163d4-9e19-4fa7-9be6-000c61aad77a

Title: CobaltStrike Named Pipe
- description: Detects the creation of a named pipe as used by CobaltStrike
- category: data/rules/windows/pipe_created
- level: critical
- id: d5601f8c-b26f-4ab0-9035-69e11a8d4ad2

Title: Browser Credential Store Access
- description: Detects suspicious processes based on name and location that access the browser credential stores which can be
- category: data/rules/windows/file_access
- level: medium
- id: 91cb43db-302a-47e3-b3c8-7ede481e27bf

Title: LSASS Access from Program in Suspicious Folder
- description: Detects process access to LSASS memory with suspicious access flags and from a suspicious folder
- category: data/rules/windows/process_access
- level: high
- id: fa34b441-961a-42fa-a100-ecc28c886725

Title: UAC Bypass Using WOW64 Logger DLL Hijack
- description: Detects the pattern of UAC Bypass using a WoW64 logger DLL hijack (UACMe 30)
- category: data/rules/windows/process_access
- level: high
- id: 4f6c43e2-f989-4ea5-bcd8-843b49a0317c

Title: CobaltStrike BOF Injection Pattern
- description: Detects a typical pattern of a CobaltStrike BOF which inject into other processes
- category: data/rules/windows/process_access
- level: high
- id: 09706624-b7f6-455d-9d02-adee024cee1d

Title: Malware Shellcode in Verclsid Target Process
- description: Detects a process access to verclsid.exe that injects shellcode from a Microsoft Office application / VBA macro
- category: data/rules/windows/process_access
- level: high
- id: b7967e22-3d7e-409b-9ed5-cdae3f9243a1

Title: LSASS Memory Dump
- description: Detects process LSASS memory dump using Mimikatz, NanoDump, Invoke-Mimikatz, Procdump or Taskmgr based on the C
- category: data/rules/windows/process_access
- level: high
- id: 5ef9853e-4d0e-4a70-846f-a9ca37d876da

Title: CMSTP Execution Process Access
- description: Detects various indicators of Microsoft Connection Manager Profile Installer execution
- category: data/rules/windows/process_access
- level: high
- id: 3b4b232a-af90-427c-a22f-30b0c0837b95

Title: Lsass Memory Dump via Comsvcs DLL
- description: Detects adversaries leveraging the MiniDump export function from comsvcs.dll via rundll32 to perform a memory d
- category: data/rules/windows/process_access
- level: critical
- id: a49fa4d5-11db-418c-8473-1e014a8dd462

Title: LSASS Access from White-Listed Processes
- description: Detects a possible process memory dump that uses the white-listed filename like TrolleyExpress.exe as a way to
- category: data/rules/windows/process_access
- level: high
- id: 4be8b654-0c01-4c9d-a10c-6b28467fc651

Title: LittleCorporal Generated Maldoc Injection
- description: Detects the process injection of a LittleCorporal generated Maldoc.
- category: data/rules/windows/process_access
- level: high
- id: 7bdde3bf-2a42-4c39-aa31-a92b3e17afac

Title: Direct Syscall of NtOpenProcess
- description: Detects the usage of the direct syscall of NtOpenProcess which might be done from a CobaltStrike BOF.
- category: data/rules/windows/process_access
- level: critical
- id: 3f3f3506-1895-401b-9cc3-e86b16e630d0

Title: Suspicious In-Memory Module Execution
- description: Detects the access to processes by other suspicious processes which have reflectively loaded libraries in their
- category: data/rules/windows/process_access
- level: low
- id: 5f113a8f-8b61-41ca-b90f-d374fa7e4a39

Title: Suspect Svchost Memory Asccess
- description: Detects suspect access to svchost process memory such as that used by Invoke-Phantom to kill the winRM windows
- category: data/rules/windows/process_access
- level: high
- id: 166e9c50-8cd9-44af-815d-d1f0c0e90dde

Title: Suspicious GrantedAccess Flags on LSASS Access
- description: Detects process access to LSASS memory with suspicious access flags
- category: data/rules/windows/process_access
- level: high
- id: a18dd26b-6450-46de-8c91-9659150cf088

Title: Credentials Dumping Tools Accessing LSASS Memory
- description: Detects process access LSASS memory which is typical for credentials dumping tools

- category: data/rules/windows/process_access
- level: high
- id: 32d0d3e2-e58d-4d41-926b-18b520b2b32d

Title: LSASS Memory Access by Tool Named Dump
- description: Detects a possible process memory dump based on a keyword in the file name of the accessing process
- category: data/rules/windows/process_access
- level: high
- id: 9bd012ee-0dff-44d7-84a0-aa698cfd87a3

Title: Rare GrantedAccess Flags on LSASS Access
- description: Detects process access to LSASS memory with suspicious access flags 0x410 and 0x01410 (spin-off of similar rule
- category: data/rules/windows/process_access
- level: medium
- id: 678dfc63-fefb-47a5-a04c-26bcf8cc9f65

Title: Credential Dumping by LaZagne
- description: Detects LSASS process access by LaZagne for credential dumping.
- category: data/rules/windows/process_access
- level: critical
- id: 4b9a8556-99c4-470b-a40c-9c8d02c77ed0

Title: SVCHOST Credential Dump
- description: Detects when a process, such as mimikatz, accesses the memory of svchost to dump credentials
- category: data/rules/windows/process_access
- level: critical
- id: 174afcfa-6e40-4ae9-af64-496546389294

Title: Load Undocumented Autoelevated COM Interface
- description: COM interface (EditionUpgradeManager) that is not used by standard executables.
- category: data/rules/windows/process_access
- level: high
- id: fb3722e4-1a06-46b6-b772-253e2e7db933

Title: Credential Dumping by Pypykatz
- description: Detects LSASS process access by pypykatz for credential dumping.
- category: data/rules/windows/process_access
- level: critical
- id: 7186e989-4ed7-4f4e-a656-4674b9e3e48b

Title: Shellcode Injection
- description: Detects shellcode injection by Metasploit's migrate and Empire's psinject
- category: data/rules/windows/process_access
- level: high
- id: 250ae82f-736e-4844-a68b-0b5e8cc887da

Title: Mimikatz through Windows Remote Management
- description: Detects usage of mimikatz through WinRM protocol by monitoring access to lsass process by wsmprovhost.exe.
- category: data/rules/windows/process_access
- level: high
- id: aa35a627-33fb-4d04-a165-d33b4afca3e8

Title: Accessing WinAPI in PowerShell for Credentials Dumping
- description: Detects Accessing to lsass.exe by Powershell
- category: data/rules/windows/sysmon
- level: high
- id: 3f07b9d1-2082-4c56-9277-613a621983cc

Title: Sysmon Configuration Modification
- description: Someone try to hide from Sysmon
- category: data/rules/windows/sysmon
- level: high
- id: 1f2b5353-573f-4880-8e33-7d04dcf97744

Title: Sysmon Configuration Change
- description: Detects a Sysmon configuration change, which could be the result of a legitimate reconfiguration or someone try
- category: data/rules/windows/sysmon
- level: medium
- id: 8ac03a65-6c84-4116-acad-dc1558ff7a77

Title: Sysmon Configuration Error
- description: Someone try to hide from Sysmon
- category: data/rules/windows/sysmon
- level: high
- id: 815cd91b-7dbc-4247-841a-d7dd1392b0a8

Title: Sysmon Process Hollowing Detection
- description: Detects when a memory process image does not match the disk image, indicative of process hollowing.
- category: data/rules/windows/sysmon
- level: high
- id: c4b890e5-8d8c-4496-8c66-c805753817cd

Title: T1021 DCOM InternetExplorer.Application Iertutil DLL Hijack
- description: Detects a threat actor creating a file named `iertutil.dll` in the `C:\Program Files\Internet Explorer\` direct
- category: data/rules/windows/sysmon
- level: critical
- id: e554f142-5cf3-4e55-ace9-a1b59e0def65

Title: Renamed Powershell Under Powershell Channel
- description: Detects renamed powershell
- category: data/rules/windows/powershell/powershell_classic
- level: low
- id: 30a8cb77-8eb3-4cfb-8e79-ad457c5a4592

Title: Suspicious Non PowerShell WSMAN COM Provider
- description: Detects suspicious use of the WSMAN provider without PowerShell.exe as the host application.
- category: data/rules/windows/powershell/powershell_classic
- level: medium
- id: df9a0e0e-fedb-4d6c-8668-d765dfc92aa7

Title: Zip A Folder With PowerShell For Staging In Temp
- description: Use living off the land tools to zip a file and stage it in the Windows temporary folder for later exfiltration
- category: data/rules/windows/powershell/powershell_classic
- level: medium
- id: 71ff406e-b633-4989-96ec-bc49d825a412

Title: Suspicious PowerShell Download
- description: Detects suspicious PowerShell download command
- category: data/rules/windows/powershell/powershell_classic
- level: medium
- id: 3236fcd0-b7e3-4433-b4f8-86ad61a9af2d

Title: Suspicious XOR Encoded PowerShell Command Line
- description: Detects suspicious powershell process which includes bxor command, alternative obfuscation method to b64 encode
- category: data/rules/windows/powershell/powershell_classic
- level: medium
- id: 812837bb-b17f-45e9-8bd0-0ec35d2e3bd6

Title: Netcat The Powershell Version
- description: Adversaries may use a non-application layer protocol for communication between host and C2 server or among infe
- category: data/rules/windows/powershell/powershell_classic
- level: medium
- id: c5b20776-639a-49bf-94c7-84f912b91c15

Title: Use Get-NetTCPConnection
- description: Adversaries may attempt to get a listing of network connections to or from the compromised system they are curr
- category: data/rules/windows/powershell/powershell_classic
- level: low
- id: b366adb4-d63d-422d-8a2c-186463b5ded0

Title: PowerShell Downgrade Attack
- description: Detects PowerShell downgrade attack by comparing the host versions with the actually used engine version 2.0
- category: data/rules/windows/powershell/powershell_classic
- level: medium
- id: 6331d09b-4785-4c13-980f-f96661356249

Title: Tamper Windows Defender
- description: Attempting to disable scheduled scanning and other parts of windows defender atp.

- category: data/rules/windows/powershell/powershell_classic
- level: high
- id: ec19ebab-72dc-40e1-9728-4c0b805d722c

Title: Remote PowerShell Session
- description: Detects remote PowerShell sessions
- category: data/rules/windows/powershell/powershell_classic
- level: high
- id: 60167e5c-84b2-4c95-a7ac-86281f27c445

Title: Abusable Invoke-ATHRemoteFXvGPUDisablementCommand
- description: RemoteFXvGPUDisablement.exe is an abusable, signed PowerShell host executable that was introduced in Windows 10
- category: data/rules/windows/powershell/powershell_classic
- level: medium
- id: f65e22f9-819e-4f96-9c7b-498364ae7a25

Title: Delete Volume Shadow Copies Via WMI With PowerShell
- description: Shadow Copies deletion using operating systems utilities via PowerShell
- category: data/rules/windows/powershell/powershell_classic
- level: critical
- id: 87df9ee1-5416-453a-8a08-e8d4a51e9ce1

Title: PowerShell Called from an Executable Version Mismatch
- description: Detects PowerShell called from an executable by the version mismatch method
- category: data/rules/windows/powershell/powershell_classic
- level: high
- id: c70e019b-1479-4b65-b0cc-cd0c6093a599

Title: Alternate PowerShell Hosts
- description: Detects alternate PowerShell hosts potentially bypassing detections looking for powershell.exe
- category: data/rules/windows/powershell/powershell_classic
- level: medium
- id: d7326048-328b-4d5e-98af-86e84b17c765

Title: Alternate PowerShell Hosts
- description: Detects alternate PowerShell hosts potentially bypassing detections looking for powershell.exe
- category: data/rules/windows/powershell/powershell_module
- level: medium
- id: 64e8e417-c19a-475a-8d19-98ea705394cc

Title: Zip A Folder With PowerShell For Staging In Temp
- description: Use living off the land tools to zip a file and stage it in the Windows temporary folder for later exfiltration
- category: data/rules/windows/powershell/powershell_module
- level: medium
- id: daf7eb81-35fd-410d-9d7a-657837e602bb

Title: Remote PowerShell Session
- description: Detects remote PowerShell sessions
- category: data/rules/windows/powershell/powershell_module
- level: high
- id: 96b9f619-aa91-478f-bacb-c3e50f8df575

Title: Invoke-Obfuscation CLIP+ Launcher
- description: Detects Obfuscated use of Clip.exe to execute PowerShell
- category: data/rules/windows/powershell/powershell_module
- level: high
- id: a136cde0-61ad-4a61-9b82-8dc490e60dd2

Title: Use Get-NetTCPConnection
- description: Adversaries may attempt to get a listing of network connections to or from the compromised system they are curr
- category: data/rules/windows/powershell/powershell_module
- level: low
- id: aff815cc-e400-4bf0-a47a-5d8a2407d4e1

Title: Invoke-Obfuscation RUNDLL LAUNCHER
- description: Detects Obfuscated Powershell via RUNDLL LAUNCHER
- category: data/rules/windows/powershell/powershell_module
- level: medium
- id: a23791fe-8846-485a-b16b-ca691e1b03d4

Title: Invoke-Obfuscation Via Use Clip
- description: Detects Obfuscated Powershell via use Clip.exe in Scripts
- category: data/rules/windows/powershell/powershell_module
- level: high
- id: ebdf49d8-b89c-46c9-8fdf-2c308406f6bd

Title: Invoke-Obfuscation Via Use MSHTA
- description: Detects Obfuscated Powershell via use MSHTA in Scripts
- category: data/rules/windows/powershell/powershell_module
- level: high
- id: 07ad2ea8-6a55-4ac6-bf3e-91b8e59676eb

Title: Clear PowerShell History
- description: Detects keywords that could indicate clearing PowerShell history
- category: data/rules/windows/powershell/powershell_module
- level: medium
- id: f99276ad-d122-4989-a09a-d00904a5f9d2

Title: Invoke-Obfuscation COMPRESS OBFUSCATION
- description: Detects Obfuscated Powershell via COMPRESS OBFUSCATION
- category: data/rules/windows/powershell/powershell_module
- level: medium
- id: 7034cbbb-cc55-4dc2-8dad-36c0b942e8f1

Title: Suspicious Get Information for SMB Share
- description: Adversaries may look for folders and drives shared on remote systems as a means of identifying sources of infor

to identify potential systems of interest for Lateral Movement. Networks often contain shared network drives and folders that enable users to access file directories on various systems across a network.

- category: data/rules/windows/powershell/powershell_module
- level: low
- id: 6942bd25-5970-40ab-af49-944247103358

Title: Invoke-Obfuscation Obfuscated IEX Invocation
- description: Detects all variations of obfuscated powershell IEX invocation code generated by Invoke-Obfuscation framework f
- category: data/rules/windows/powershell/powershell_module
- level: high
- id: 2f211361-7dce-442d-b78a-c04039677378

Title: Invoke-Obfuscation Via Use Rundll32
- description: Detects Obfuscated Powershell via use Rundll32 in Scripts
- category: data/rules/windows/powershell/powershell_module
- level: high
- id: 88a22f69-62f9-4b8a-aa00-6b0212f2f05a

Title: Suspicious PowerShell Invocations - Specific
- description: Detects suspicious PowerShell invocation command parameters
- category: data/rules/windows/powershell/powershell_module
- level: high
- id: 8ff28fdd-e2fa-4dfa-aeda-ef3d61c62090

Title: Suspicious Get Local Groups Information
- description: Adversaries may attempt to find local system groups and permission settings.

The knowledge of local system permission groups can help adversaries determine which groups exist and which users belong to a particular group. Adversaries may use this information to determine which users have elevated permissions, such as the users found within the local administrators group.

- category: data/rules/windows/powershell/powershell_module
- level: low
- id: cef24b90-dddc-4ae1-a09a-8764872f69fc

Title: Invoke-Obfuscation VAR++ LAUNCHER OBFUSCATION
- description: Detects Obfuscated Powershell via VAR++ LAUNCHER
- category: data/rules/windows/powershell/powershell_module
- level: high
- id: f3c89218-8c3d-4ba9-9974-f1d8e6a1b4a6

Title: Invoke-Obfuscation VAR+ Launcher

- description: Detects Obfuscated use of Environment Variables to execute PowerShell
- category: data/rules/windows/powershell/powershell_module
- level: high
- id: 6bfb8fa7-b2e7-4f6c-8d9d-824e5d06ea9e

Title: Bad Opsec Powershell Code Artifacts
- description: Focuses on trivial artifacts observed in variants of prevalent offensive ps1 payloads, including Cobalt Strike
- category: data/rules/windows/powershell/powershell_module
- level: critical
- id: 8d31a8ce-46b5-4dd6-bdc3-680931f1db86

Title: Netcat The Powershell Version
- description: Adversaries may use a non-application layer protocol for communication between host and C2 server or among infe
- category: data/rules/windows/powershell/powershell_module
- level: medium
- id: bf7286e7-c0be-460b-a7e8-5b2e07ecc2f2

Title: Suspicious Computer Machine Password by PowerShell
- description: The Reset-ComputerMachinePassword cmdlet changes the computer account password that the computers use to authen
- category: data/rules/windows/powershell/powershell_module
- level: medium
- id: e3818659-5016-4811-a73c-dde4679169d2

Title: SyncAppvPublishingServer Execution to Bypass Powershell Restriction
- description: Detects SyncAppvPublishingServer process execution which usually utilized by adversaries to bypass PowerShell e
- category: data/rules/windows/powershell/powershell_module
- level: medium
- id: fe5ce7eb-dad8-467c-84a9-31ec23bd644a

Title: Suspicious PowerShell Invocations - Generic
- description: Detects suspicious PowerShell invocation command parameters
- category: data/rules/windows/powershell/powershell_module
- level: high
- id: bbb80e91-5746-4fbe-8898-122e2cafdbf4

Title: Abusable Invoke-ATHRemoteFXvGPUDisablementCommand
- description: RemoteFXvGPUDisablement.exe is an abusable, signed PowerShell host executable that was introduced in Windows 10
- category: data/rules/windows/powershell/powershell_module
- level: medium
- id: 38a7625e-b2cb-485d-b83d-aff137d859f4

Title: PowerShell Get Clipboard
- description: A General detection for the Get-Clipboard commands in PowerShell logs. This could be an adversary capturing cli
- category: data/rules/windows/powershell/powershell_module
- level: medium
- id: 4cbd4f12-2e22-43e3-882f-bff3247ffb78

Title: Invoke-Obfuscation Via Stdin
- description: Detects Obfuscated Powershell via Stdin in Scripts
- category: data/rules/windows/powershell/powershell_module
- level: high
- id: c72aca44-8d52-45ad-8f81-f96c4d3c755e

Title: Suspicious PowerShell Download
- description: Detects suspicious PowerShell download command
- category: data/rules/windows/powershell/powershell_module
- level: medium
- id: de41232e-12e8-49fa-86bc-c05c7e722df9

Title: PowerShell Decompress Commands
- description: A General detection for specific decompress commands in PowerShell logs. This could be an adversary decompressi
- category: data/rules/windows/powershell/powershell_module
- level: informational
- id: 1ddc1472-8e52-4f7d-9f11-eab14fc171f5

Title: Invoke-Obfuscation STDIN+ Launcher
- description: Detects Obfuscated use of stdin to execute PowerShell
- category: data/rules/windows/powershell/powershell_module
- level: high

- id: 9ac8b09b-45de-4a07-9da1-0de8c09304a3

Title: Suspicious Get-ADDBAccount Usage
- description: Detects suspicious invocation of the Get-ADDBAccount script that reads from a ntds.dit file and may be used to
- category: data/rules/windows/powershell/powershell_module
- level: high
- id: b140afd9-474b-4072-958e-2ebb435abd68

Title: Suspicious Get Information for AD Groups or DoesNotRequirePreAuth User
- description: Adversaries may attempt to find domain-level groups and permission settings.

The knowledge of domain-level permission groups can help adversaries determine which groups exist and which users belong to a particular group. Adversaries may use this information to determine which users have elevated permissions, such as domain administrators.

- category: data/rules/windows/powershell/powershell_module
- level: low
- id: 815bfc17-7fc6-4908-a55e-2f37b98cedb4

Title: Malicious PowerShell Keywords
- description: Detects keywords from well-known PowerShell exploitation frameworks
- category: data/rules/windows/powershell/powershell_script
- level: high
- id: f62176f3-8128-4faa-bf6c-83261322e5eb

Title: Testing Usage of Uncommonly Used Port
- description: Adversaries may communicate using a protocol and port paring that are typically not associated.

For example, HTTPS over port 8088(Citation: Symantec Elfin Mar 2019) or port 587(Citation: Fortinet Agent Tesla April 2018) as opposed to the traditional port 443.

- category: data/rules/windows/powershell/powershell_script
- level: medium
- id: adf876b3-f1f8-4aa9-a4e4-a64106feec06

Title: Windows PowerShell Web Request
- description: Detects the use of various web request methods (including aliases) via Windows PowerShell command
- category: data/rules/windows/powershell/powershell_script
- level: medium
- id: 1139d2e2-84b1-4226-b445-354492eba8ba

Title: Service Registry Permissions Weakness Check
- description: Adversaries may execute their own malicious payloads by hijacking the Registry entries used by services.

Adversaries may use flaws in the permissions for registry to redirect from the originally specified executable to one that they control, in order to launch their own code at Service start. Windows stores local service configuration information in the Registry under HKLM\SYSTEM\CurrentControlSet\Services

- category: data/rules/windows/powershell/powershell_script
- level: medium
- id: 95afc12e-3cbb-40c3-9340-84a032e596a3

Title: Suspicious Get Information for AD Groups or DoesNotRequirePreAuth User
- description: Adversaries may attempt to find domain-level groups and permission settings.

The knowledge of domain-level permission groups can help adversaries determine which groups exist and which users belong to a particular group. Adversaries may use this information to determine which users have elevated permissions, such as domain administrators.

- category: data/rules/windows/powershell/powershell_script
- level: low
- id: 88f0884b-331d-403d-a3a1-b668cf035603

Title: Data Compressed - PowerShell
- description: An adversary may compress data (e.g., sensitive documents) that is collected prior to exfiltration in order to
- category: data/rules/windows/powershell/powershell_script
- level: low
- id: 6dc5d284-69ea-42cf-9311-fb1c3932a69a

Title: WMImplant Hack Tool
- description: Detects parameters used by WMImplant
- category: data/rules/windows/powershell/powershell_script
- level: high

```
- id: 8028c2c3-e25a-46e3-827f-bbb5abf181d7

Title: Change PowerShell Policies to an Unsecure Level
- description: Detects use of Set-ExecutionPolicy to set a unsecure policies
- category: data/rules/windows/powershell/powershell_script
- level: medium
- id: 61d0475c-173f-4844-86f7-f3eebae1c66b

Title: Suspicious PowerShell Keywords
- description: Detects keywords that could indicate the use of some PowerShell exploitation framework
- category: data/rules/windows/powershell/powershell_script
- level: high
- id: 1f49f2ab-26bc-48b3-96cc-dcffbc93eadf

Title: Powershell Execute Batch Script
- description: Adversaries may abuse the Windows command shell for execution.
```

The Windows command shell (cmd) is the primary command prompt on Windows systems. The Windows command prompt can be used to control almost any aspect of a system, with various permission levels required for different subsets of commands. Batch files (ex: .bat or .cmd) also provide the shell with a list of sequential commands to run, as well as normal scripting operations such as conditionals and loops. Common uses of batch files include long or repetitive tasks, or the need to run the same set of commands on multiple system

```
- category: data/rules/windows/powershell/powershell_script
- level: medium
- id: b5522a23-82da-44e5-9c8b-e10ed8955f88

Title: Suspicious IO.FileStream
- description: Open a handle on the drive volume via the \\.\ DOS device path specifier and perform direct access read of the
- category: data/rules/windows/powershell/powershell_script
- level: medium
- id: 70ad982f-67c8-40e0-a955-b920c2fa05cb

Title: PowerShell Remote Session Creation
- description: Adversaries may abuse PowerShell commands and scripts for execution.
```

PowerShell is a powerful interactive command-line interface and scripting environment included in the Windows operating system

```
- category: data/rules/windows/powershell/powershell_script
- level: medium
- id: a0edd39f-a0c6-4c17-8141-261f958e8d8f

Title: Accessing WinAPI in PowerShell
- description: Detecting use WinAPI Functions in PowerShell
- category: data/rules/windows/powershell/powershell_script
- level: high
- id: 03d83090-8cba-44a0-b02f-0b756a050306

Title: Invoke-Obfuscation Obfuscated IEX Invocation
- description: Detects all variations of obfuscated powershell IEX invocation code generated by Invoke-Obfuscation framework f
- category: data/rules/windows/powershell/powershell_script
- level: high
- id: 1b9dc62e-6e9e-42a3-8990-94d7a10007f7

Title: PowerShell Deleted Mounted Share
- description: Detects when when a mounted share is removed. Adversaries may remove share connections that are no longer usefu
- category: data/rules/windows/powershell/powershell_script
- level: medium
- id: 66a4d409-451b-4151-94f4-a55d559c49b0

Title: Automated Collection Command PowerShell
- description: Once established within a system or network, an adversary may use automated techniques for collecting internal
- category: data/rules/windows/powershell/powershell_script
- level: medium
- id: c1dda054-d638-4c16-afc8-53e007f3fbc5

Title: Invoke-Obfuscation CLIP+ Launcher
- description: Detects Obfuscated use of Clip.exe to execute PowerShell
- category: data/rules/windows/powershell/powershell_script
- level: high
- id: 73e67340-0d25-11eb-adc1-0242ac120002
```

```
Title: Zip A Folder With PowerShell For Staging In Temp
- description: Use living off the land tools to zip a file and stage it in the Windows temporary folder for later exfiltration
- category: data/rules/windows/powershell/powershell_script
- level: medium
- id: b7a3c9a3-09ea-4934-8864-6a32cacd98d9

Title: Invoke-Obfuscation STDIN+ Launcher
- description: Detects Obfuscated use of stdin to execute PowerShell
- category: data/rules/windows/powershell/powershell_script
- level: high
- id: 779c8c12-0eb1-11eb-adc1-0242ac120002

Title: Powershell Create Scheduled Task
- description: Adversaries may abuse the Windows Task Scheduler to perform task scheduling for initial or recurring execution
- category: data/rules/windows/powershell/powershell_script
- level: medium
- id: 363eccc0-279a-4ccf-a3ab-24c2e63b11fb

Title: Replace Desktop Wallpaper by Powershell
- description: An adversary may deface systems internal to an organization in an attempt to intimidate or mislead users.
```

This may take the form of modifications to internal websites, or directly to user systems with the replacement of the desktop wallpaper

```
- category: data/rules/windows/powershell/powershell_script
- level: low
- id: c5ac6a1e-9407-45f5-a0ce-ca9a0806a287

Title: Windows Screen Capture with CopyFromScreen
- description: Adversaries may attempt to take screen captures of the desktop to gather information over the course of an oper
```

Screen capturing functionality may be included as a feature of a remote access tool used in post-compromise operations

```
- category: data/rules/windows/powershell/powershell_script
- level: medium
- id: d4a11f63-2390-411c-9adf-d791fd152830

Title: Invoke-Obfuscation VAR+ Launcher
- description: Detects Obfuscated use of Environment Variables to execute PowerShell
- category: data/rules/windows/powershell/powershell_script
- level: high
- id: 0adfbc14-0ed1-11eb-adc1-0242ac120002

Title: Powershell File and Directory Discovery
- description: Adversaries may enumerate files and directories or may search in specific locations of a host or network share
```

Adversaries may use the information from File and Directory Discovery during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions.

```
- category: data/rules/windows/powershell/powershell_script
- level: low
- id: d23f2ba5-9da0-4463-8908-8ee47f614bb9

Title: Invoke-Obfuscation VAR++ LAUNCHER OBFUSCATION
- description: Detects Obfuscated Powershell via VAR++ LAUNCHER
- category: data/rules/windows/powershell/powershell_script
- level: high
- id: e54f5149-6ba3-49cf-b153-070d24679126

Title: Powershell Trigger Profiles by Add_Content
- description: Adversaries may gain persistence and elevate privileges by executing malicious content triggered by PowerShell
- category: data/rules/windows/powershell/powershell_script
- level: medium
- id: 05b3e303-faf0-4f4a-9b30-46cc13e69152

Title: Suspicious Get Local Groups Information
- description: Adversaries may attempt to find local system groups and permission settings.
```

The knowledge of local system permission groups can help adversaries determine which groups exist and which users belong to a particular group. Adversaries may use this information to determine which users have elevated permissions, such as the users found within the local administrators group.

- category: data/rules/windows/powershell/powershell_script
- level: low
- id: fa6a5a45-3ee2-4529-aa14-ee5edc9e29cb

Title: Access to Browser Login Data
- description: Adversaries may acquire credentials from web browsers by reading files specific to the target browser.

Web browsers commonly save credentials such as website usernames and passwords so that they do not need to be entered manually in the future. Web browsers typically store the credentials in an encrypted format within a credential store.

- category: data/rules/windows/powershell/powershell_script
- level: medium
- id: fc028194-969d-4122-8abe-0470d5b8f12f

Title: Suspicious Connection to Remote Account
- description: Adversaries with no prior knowledge of legitimate credentials within the system or environment may guess passwo

Without knowledge of the password for an account, an adversary may opt to systematically guess the password using a repetitive or iterative mechanism

- category: data/rules/windows/powershell/powershell_script
- level: low
- id: 1883444f-084b-419b-ac62-e0d0c5b3693f

Title: PowerShell ICMP Exfiltration
- description: Detects Exfiltration Over Alternative Protocol - ICMP. Adversaries may steal data by exfiltrating it over an un
- category: data/rules/windows/powershell/powershell_script
- level: medium
- id: 4c4af3cd-2115-479c-8193-6b8bfce9001c

Title: Powershell Suspicious Win32_PnPEntity
- description: Adversaries may attempt to gather information about attached peripheral devices and components connected to a c
- category: data/rules/windows/powershell/powershell_script
- level: low
- id: b26647de-4feb-4283-af6b-6117661283c5

Title: Recon Information for Export with PowerShell
- description: Once established within a system or network, an adversary may use automated techniques for collecting internal
- category: data/rules/windows/powershell/powershell_script
- level: medium
- id: a9723fcc-881c-424c-8709-fd61442ab3c3

Title: Powershell DNSExfiltration
- description: DNSExfiltrator allows for transfering (exfiltrate) a file over a DNS request covert channel
- category: data/rules/windows/powershell/powershell_script
- level: high
- id: d59d7842-9a21-4bc6-ba98-64bfe0091355

Title: Execution via CL_Invocation.ps1
- description: Detects Execution via SyncInvoke in CL_Invocation.ps1 module
- category: data/rules/windows/powershell/powershell_script
- level: high
- id: 4cd29327-685a-460e-9dac-c3ab96e549dc

Title: Manipulation of User Computer or Group Security Principals Across AD
- description: Adversaries may create a domain account to maintain access to victim systems.

Domain accounts are those managed by Active Directory Domain Services where access and permissions are configured across systems and services that are part of that domain..

- category: data/rules/windows/powershell/powershell_script
- level: medium
- id: b29a93fb-087c-4b5b-a84d-ee3309e69d08

Title: Invoke-Obfuscation Via Stdin
- description: Detects Obfuscated Powershell via Stdin in Scripts
- category: data/rules/windows/powershell/powershell_script
- level: high
- id: 86b896ba-ffa1-4fea-83e3-ee28a4c915c7

Title: Security Software Discovery by Powershell

- description: Adversaries may attempt to get a listing of security software, configurations, defensive tools, and sensors tha

This may include things such as firewall rules and anti-viru

- category: data/rules/windows/powershell/powershell_script
- level: low
- id: 904e8e61-8edf-4350-b59c-b905fc8e810c

Title: Windows Firewall Profile Disabled
- description: Detects when a user disables the Windows Firewall via a Profile to help evade defense.
- category: data/rules/windows/powershell/powershell_script
- level: high
- id: 488b44e7-3781-4a71-888d-c95abfacf44d

Title: Invoke-Obfuscation Via Use MSHTA
- description: Detects Obfuscated Powershell via use MSHTA in Scripts
- category: data/rules/windows/powershell/powershell_script
- level: high
- id: e55a5195-4724-480e-a77e-3ebe64bd3759

Title: Invoke-Obfuscation Via Use Clip
- description: Detects Obfuscated Powershell via use Clip.exe in Scripts
- category: data/rules/windows/powershell/powershell_script
- level: high
- id: db92dd33-a3ad-49cf-8c2c-608c3e30ace0

Title: Powershell Directory Enumeration
- description: Detects technique used by MAZE ransomware to enumerate directories using Powershell
- category: data/rules/windows/powershell/powershell_script
- level: medium
- id: 162e69a7-7981-4344-84a9-0f1c9a217a52

Title: PowerShell Credential Prompt
- description: Detects PowerShell calling a credential prompt
- category: data/rules/windows/powershell/powershell_script
- level: high
- id: ca8b77a9-d499-4095-b793-5d5f330d450e

Title: Suspicious GetTypeFromCLSID ShellExecute
- description: Detects suspicious Powershell code that execute COM Objects
- category: data/rules/windows/powershell/powershell_script
- level: medium
- id: 8bc063d5-3a3a-4f01-a140-bc15e55e8437

Title: PowerShell ShellCode
- description: Detects Base64 encoded Shellcode
- category: data/rules/windows/powershell/powershell_script
- level: critical
- id: 16b37b70-6fcf-4814-a092-c36bd3aafcbd

Title: Suspicious Start-Process PassThru
- description: Powershell use PassThru option to start in background
- category: data/rules/windows/powershell/powershell_script
- level: medium
- id: 0718cd72-f316-4aa2-988f-838ea8533277

Title: Windows PowerShell Upload Web Request
- description: Detects the use of various web request POST or PUT methods (including aliases) via Windows PowerShell command
- category: data/rules/windows/powershell/powershell_script
- level: medium
- id: d2e3f2f6-7e09-4bf2-bc5d-90186809e7fb

Title: Suspicious PowerShell Get Current User
- description: Detects the use of PowerShell to identify the current logged user.
- category: data/rules/windows/powershell/powershell_script
- level: low
- id: 4096a49c-7de4-4da0-a230-c66ccd56ea5a

Title: Malicious PowerShell Commandlets

- description: Detects Commandlet names from well-known PowerShell exploitation frameworks
- category: data/rules/windows/powershell/powershell_script
- level: high
- id: 89819aa4-bbd6-46bc-88ec-c7f7fe30efa6

Title: Password Policy Discovery With Get-AdDefaultDomainPasswordPolicy
- description: Detetcts PowerShell activity in which Get-Addefaultdomainpasswordpolicy is used to get the default password pol
- category: data/rules/windows/powershell/powershell_script
- level: low
- id: bbb9495b-58fc-4016-b9df-9a3a1b67ca82

Title: Change User Agents with WebRequest
- description: Adversaries may communicate using application layer protocols associated with web traffic to avoid detection/ne

Commands to the remote system, and often the results of those commands, will be embedded within the protocol traffic between the client and server.

- category: data/rules/windows/powershell/powershell_script
- level: medium
- id: d4488827-73af-4f8d-9244-7b7662ef046e

Title: Clearing Windows Console History
- description: Identifies when a user attempts to clear console history. An adversary may clear the command history of a compr
- category: data/rules/windows/powershell/powershell_script
- level: high
- id: bde47d4b-9987-405c-94c7-b080410e8ea7

Title: Clear PowerShell History
- description: Detects keywords that could indicate clearing PowerShell history
- category: data/rules/windows/powershell/powershell_script
- level: medium
- id: 26b692dc-1722-49b2-b496-a8258aa6371d

Title: Powershell XML Execute Command
- description: Adversaries may abuse PowerShell commands and scripts for execution.

PowerShell is a powerful interactive command-line interface and scripting environment included in the Windows operating system. (Citation: TechNet PowerShell) Adversaries can use PowerShell to perform a number of actions, including discovery of information and execution of code

- category: data/rules/windows/powershell/powershell_script
- level: medium
- id: 6c6c6282-7671-4fe9-a0ce-a2dcebdc342b

Title: Automated Collection Bookmarks Using Get-ChildItem PowerShell
- description: Adversaries may enumerate browser bookmarks to learn more about compromised hosts.

Browser bookmarks may reveal personal information about users (ex: banking sites, interests, social media, etc.) as well as details about internal network resources such as servers, tools/dashboards, or other related infrastructure.

- category: data/rules/windows/powershell/powershell_script
- level: low
- id: e0565f5d-d420-4e02-8a68-ac00d864f9cf

Title: Remove Account From Domain Admin Group
- description: Adversaries may interrupt availability of system and network resources by inhibiting access to accounts utilize

Accounts may be deleted, locked, or manipulated (ex: changed credentials) to remove access to accounts.

- category: data/rules/windows/powershell/powershell_script
- level: medium
- id: 48a45d45-8112-416b-8a67-46e03a4b2107

Title: Suspicious Mount-DiskImage
- description: Adversaries may abuse container files such as disk image (.iso, .vhd) file formats to deliver malicious payload
- category: data/rules/windows/powershell/powershell_script
- level: low
- id: 29e1c216-6408-489d-8a06-ee9d151ef819

Title: Invoke-Obfuscation COMPRESS OBFUSCATION
- description: Detects Obfuscated Powershell via COMPRESS OBFUSCATION
- category: data/rules/windows/powershell/powershell_script

- level: medium
- id: 20e5497e-331c-4cd5-8d36-935f6e2a9a07

Title: PowerShell Get-Process LSASS in ScriptBlock
- description: Detects a Get-Process command on lsass process, which is in almost all cases a sign of malicious activity
- category: data/rules/windows/powershell/powershell_script
- level: high
- id: 84c174ab-d3ef-481f-9c86-a50d0b8e3edb

Title: Enumerate Credentials from Windows Credential Manager With PowerShell
- description: Adversaries may search for common password storage locations to obtain user credentials.

Passwords are stored in several places on a system, depending on the operating system or application holding the credentials.

- category: data/rules/windows/powershell/powershell_script
- level: medium
- id: 603c6630-5225-49c1-8047-26c964553e0e

Title: Suspicious Enumerate Active Directory Groups with Get-AdComputer
- description: Detects the use of Get-AdGroup to enumerate Groups within Active Directory
- category: data/rules/windows/powershell/powershell_script
- level: low
- id: 8c3a6607-b7dc-4f0d-a646-ef38c00b76ee

Title: Suspicious Get Information for SMB Share
- description: Adversaries may look for folders and drives shared on remote systems as a means of identifying sources of infor

to identify potential systems of interest for Lateral Movement. Networks often contain shared network drives and folders that enable users to access file directories on various systems across a network.

- category: data/rules/windows/powershell/powershell_script
- level: low
- id: 95f0643a-ed40-467c-806b-aac9542ec5ab

Title: Code Executed Via Office Add-in XLL File
- description: Adversaries may abuse Microsoft Office add-ins to obtain persistence on a compromised system.

Office add-ins can be used to add functionality to Office programs

- category: data/rules/windows/powershell/powershell_script
- level: high
- id: 36fbec91-fa1b-4d5d-8df1-8d8edcb632ad

Title: Root Certificate Installed
- description: Adversaries may install a root certificate on a compromised system to avoid warnings when connecting to adversa
- category: data/rules/windows/powershell/powershell_script
- level: medium
- id: 42821614-9264-4761-acfc-5772c3286f76

Title: Use Remove-Item to Delete File
- description: Powershell Remove-Item with -Path to delete a file or a folder with "-Recurse"
- category: data/rules/windows/powershell/powershell_script
- level: low
- id: b8af5f36-1361-4ebe-9e76-e36128d947bf

Title: Execution via CL_Invocation.ps1 (2 Lines)
- description: Detects Execution via SyncInvoke in CL_Invocation.ps1 module
- category: data/rules/windows/powershell/powershell_script
- level: high
- id: f588e69b-0750-46bb-8f87-0e9320d57536

Title: Powershell Timestomp
- description: Adversaries may modify file time attributes to hide new or changes to existing files. Timestomping is a techniq
- category: data/rules/windows/powershell/powershell_script
- level: medium
- id: c6438007-e081-42ce-9483-b067fbef33c3

Title: Dump Credentials from Windows Credential Manager With PowerShell
- description: Adversaries may search for common password storage locations to obtain user credentials.

Passwords are stored in several places on a system, depending on the operating system or application holding the credentials.

- category: data/rules/windows/powershell/powershell_script
- level: medium
- id: 99c49d9c-34ea-45f7-84a7-4751ae6b2cbc

Title: Execute Invoke-command on Remote Host
- description: Adversaries may use Valid Accounts to interact with remote systems using Windows Remote Management (WinRM). The
- category: data/rules/windows/powershell/powershell_script
- level: medium
- id: 7b836d7f-179c-4ba4-90a7-a7e60afb48e6

Title: Invoke-Obfuscation Via Use Rundll32
- description: Detects Obfuscated Powershell via use Rundll32 in Scripts
- category: data/rules/windows/powershell/powershell_script
- level: high
- id: a5a30a6e-75ca-4233-8b8c-42e0f2037d3b

Title: Powershell MsXml COM Object
- description: Adversaries may abuse PowerShell commands and scripts for execution.

PowerShell is a powerful interactive command-line interface and scripting environment included in the Windows operating system. (Citation: TechNet PowerShell) Adversaries can use PowerShell to perform a number of actions, including discovery of information and execution of code

- category: data/rules/windows/powershell/powershell_script
- level: medium
- id: 78aa1347-1517-4454-9982-b338d6df8343

Title: Create Volume Shadow Copy with Powershell
- description: Adversaries may attempt to access or create a copy of the Active Directory domain database in order to steal cr
- category: data/rules/windows/powershell/powershell_script
- level: high
- id: afd12fed-b0ec-45c9-a13d-aa86625dac81

Title: AzureHound PowerShell Commands
- description: Detects the execution of AzureHound in PowerShell, a tool to gather data from Azure for BloodHound
- category: data/rules/windows/powershell/powershell_script
- level: high
- id: 83083ac6-1816-4e76-97d7-59af9a9ae46e

Title: Malicious Nishang PowerShell Commandlets
- description: Detects Commandlet names and arguments from the Nishang exploitation framework
- category: data/rules/windows/powershell/powershell_script
- level: high
- id: f772cee9-b7c2-4cb2-8f07-49870adc02e0

Title: Request A Single Ticket via PowerShell
- description: utilize native PowerShell Identity modules to query the domain to extract the Service Principal Names for a sin

This behavior is typically used during a kerberos or silver ticket attack. A successful execution will output the SPNs for the endpoint in question.

- category: data/rules/windows/powershell/powershell_script
- level: high
- id: a861d835-af37-4930-bcd6-5b178bfb54df

Title: Suspicious Get-WmiObject
- description: The infrastructure for management data and operations that enables local and remote management of Windows perso
- category: data/rules/windows/powershell/powershell_script
- level: low
- id: 0332a266-b584-47b4-933d-a00b103e1b37

Title: Delete Volume Shadow Copies via WMI with PowerShell
- description: Deletes Windows Volume Shadow Copies with PowerShell code and Get-WMIObject. This technique is used by numerous
- category: data/rules/windows/powershell/powershell_script
- level: high
- id: e17121b4-ef2a-4418-8a59-12fb1631fa9e

Title: Suspicious New-PSDrive to Admin Share
- description: Adversaries may use to interact with a remote network share using Server Message Block (SMB). The adversary may
- category: data/rules/windows/powershell/powershell_script

- level: medium
- id: 1c563233-030e-4a07-af8c-ee0490a66d3a

Title: Malicious PowerView PowerShell Commandlets
- description: Detects Commandlet names from PowerView of PowerSploit exploitation framework.
- category: data/rules/windows/powershell/powershell_script
- level: high
- id: dcd74b95-3f36-4ed9-9598-0490951643aa

Title: Suspicious Start-Process PassThru
- description: Attempting to disable scheduled scanning and other parts of windows defender atp. Or set default actions to all
- category: data/rules/windows/powershell/powershell_script
- level: high
- id: 14c71865-6cd3-44ae-adaa-1db923fae5f2

Title: Execution via CL_Mutexverifiers.ps1
- description: Detects Execution via runAfterCancelProcess in CL_Mutexverifiers.ps1 module
- category: data/rules/windows/powershell/powershell_script
- level: high
- id: 39776c99-1c7b-4ba0-b5aa-641525eee1a4

Title: PrintNightmare Powershell Exploitation
- description: Detects Commandlet name for PrintNightmare exploitation.
- category: data/rules/windows/powershell/powershell_script
- level: high
- id: 6d3f1399-a81c-4409-aff3-1ecfe9330baf

Title: Suspicious Get-ADReplAccount
- description: The DSInternals PowerShell Module exposes several internal features of Active Directory and Azure Active Direct
- category: data/rules/windows/powershell/powershell_script
- level: medium
- id: 060c3ef1-fd0a-4091-bf46-e7d625f60b73

Title: Suspicious Enumerate Active Directory Computers with Get-AdComputer
- description: utilize Get-AdComputer to enumerate Computers within Active Directory.
- category: data/rules/windows/powershell/powershell_script
- level: low
- id: 36bed6b2-e9a0-4fff-beeb-413a92b86138

Title: Suspicious Process Discovery With Get-Process
- description: Get the processes that are running on the local computer.
- category: data/rules/windows/powershell/powershell_script
- level: low
- id: af4c87ce-bdda-4215-b998-15220772e993

Title: Suspicious PowerShell Invocations - Specific
- description: Detects suspicious PowerShell invocation command parameters
- category: data/rules/windows/powershell/powershell_script
- level: high
- id: ae7fbf8e-f3cb-49fd-8db4-5f3bed522c71

Title: Powershell Store File In Alternate Data Stream
- description: Storing files in Alternate Data Stream (ADS) similar to Astaroth malware.
- category: data/rules/windows/powershell/powershell_script
- level: medium
- id: a699b30e-d010-46c8-bbd1-ee2e26765fe9

Title: DirectorySearcher Powershell Exploitation
- description: Enumerates Active Directory to determine computers that are joined to the domain
- category: data/rules/windows/powershell/powershell_script
- level: medium
- id: 1f6399cf-2c80-4924-ace1-6fcff3393480

Title: Powershell Detect Virtualization Environment
- description: Adversaries may employ various system checks to detect and avoid virtualization and analysis environments. This
- category: data/rules/windows/powershell/powershell_script
- level: medium
- id: d93129cd-1ee0-479f-bc03-ca6f129882e3

Title: Get-ADUser Enumeration Using UserAccountControl Flags
- description: Detects AS-REP roasting is an attack that is often-overlooked. It is not very common as you have to explicitly
- category: data/rules/windows/powershell/powershell_script
- level: medium
- id: 96c982fe-3d08-4df4-bed2-eb14e02f21c8

Title: Powershell LocalAccount Manipulation
- description: Adversaries may manipulate accounts to maintain access to victim systems.

Account manipulation may consist of any action that preserves adversary access to a compromised account, such as modifying credentials or permission groups

- category: data/rules/windows/powershell/powershell_script
- level: medium
- id: 4fdc44df-bfe9-4fcc-b041-68f5a2d3031c

Title: Malicious ShellIntel PowerShell Commandlets
- description: Detects Commandlet names from ShellIntel exploitation scripts.
- category: data/rules/windows/powershell/powershell_script
- level: high
- id: 402e1e1d-ad59-47b6-bf80-1ee44985b3a7

Title: Powershell Local Email Collection
- description: Adversaries may target user email on local systems to collect sensitive information. Files containing email dat
- category: data/rules/windows/powershell/powershell_script
- level: medium
- id: 2837e152-93c8-43d2-85ba-c3cd3c2ae614

Title: Winlogon Helper DLL
- description: Winlogon.exe is a Windows component responsible for actions at logon/logoff as well as the secure attention seq
- category: data/rules/windows/powershell/powershell_script
- level: medium
- id: 851c506b-6b7c-4ce2-8802-c703009d03c0

Title: Suspicious Hyper-V Cmdlets
- description: Adversaries may carry out malicious operations using a virtual instance to avoid detection
- category: data/rules/windows/powershell/powershell_script
- level: medium
- id: 42d36aa1-3240-4db0-8257-e0118dcdd9cd

Title: Invoke-Obfuscation RUNDLL LAUNCHER
- description: Detects Obfuscated Powershell via RUNDLL LAUNCHER
- category: data/rules/windows/powershell/powershell_script
- level: medium
- id: e6cb92b4-b470-4eb8-8a9d-d63e8583aae0

Title: Suspicious Invoke-Item From Mount-DiskImage
- description: Adversaries may abuse container files such as disk image (.iso, .vhd) file formats to deliver malicious payload
- category: data/rules/windows/powershell/powershell_script
- level: medium
- id: 902cedee-0398-4e3a-8183-6f3a89773a96

Title: Execution via CL_Mutexverifiers.ps1 (2 Lines)
- description: Detects Execution via runAfterCancelProcess in CL_Mutexverifiers.ps1 module
- category: data/rules/windows/powershell/powershell_script
- level: high
- id: 6609c444-9670-4eab-9636-fe4755a851ce

Title: Extracting Information with PowerShell
- description: Adversaries may search local file systems and remote file shares for files containing insecurely stored credent

These can be files created by users to store their own credentials, shared credential stores for a group of individuals, configuration files containing passwords for a system or service, or source code/binary files containing embedded passwords.

- category: data/rules/windows/powershell/powershell_script
- level: medium
- id: bd5971a7-626d-46ab-8176-ed643f694f68

Title: Powershell WMI Persistence
- description: Adversaries may establish persistence and elevate privileges by executing malicious content triggered by a Wind
- category: data/rules/windows/powershell/powershell_script

- level: medium
- id: 9e07f6e7-83aa-45c6-998e-0af26efd0a85

Title: Detected Windows Software Discovery
- description: Adversaries may attempt to enumerate software for a variety of reasons, such as figuring out what security meas
- category: data/rules/windows/powershell/powershell_script
- level: medium
- id: 2650dd1a-eb2a-412d-ac36-83f06c4f2282

Title: PowerShell WMI Win32_Product Install MSI
- description: Detects the execution of an MSI file using PowerShell and the WMI Win32_Product class
- category: data/rules/windows/powershell/powershell_script
- level: medium
- id: 91109523-17f0-4248-a800-f81d9e7c081d

Title: SyncAppvPublishingServer Execution to Bypass Powershell Restriction
- description: Detects SyncAppvPublishingServer process execution which usually utilized by adversaries to bypass PowerShell e
- category: data/rules/windows/powershell/powershell_script
- level: medium
- id: dddfebae-c46f-439c-af7a-fdb6bde90218

Title: Enable Windows Remote Management
- description: Adversaries may use Valid Accounts to interact with remote systems using Windows Remote Management (WinRM). The
- category: data/rules/windows/powershell/powershell_script
- level: medium
- id: 991a9744-f2f0-44f2-bd33-9092eba17dc3

Title: Suspicious PowerShell Download
- description: Detects suspicious PowerShell download command
- category: data/rules/windows/powershell/powershell_script
- level: medium
- id: 403c2cc0-7f6b-4925-9423-bfa573bed7eb

Title: Powershell Install a DLL in System32
- description: Uses PowerShell to install a DLL in System32
- category: data/rules/windows/powershell/powershell_script
- level: high
- id: 63bf8794-9917-45bc-88dd-e1b5abc0ecfd

Title: Suspicious PowerShell WindowStyle Option
- description: Adversaries may use hidden windows to conceal malicious activity from the plain sight of users. In some cases,
- category: data/rules/windows/powershell/powershell_script
- level: medium
- id: 313fbb0a-a341-4682-848d-6d6f8c4fab7c

Title: Powershell Keylogging
- description: Adversaries may log user keystrokes to intercept credentials as the user types them.
- category: data/rules/windows/powershell/powershell_script
- level: medium
- id: 34f90d3c-c297-49e9-b26d-911b05a4866c

Title: Live Memory Dump Using Powershell
- description: Detects usage of a PowerShell command to dump the live memory of a Windows machine
- category: data/rules/windows/powershell/powershell_script
- level: high
- id: cd185561-4760-45d6-a63e-a51325112cae

Title: Suspicious Export-PfxCertificate
- description: Detects Commandlet that is used to export certificates from the local certificate store and sometimes used by t
- category: data/rules/windows/powershell/powershell_script
- level: high
- id: aa7a3fce-bef5-4311-9cc1-5f04bb8c308c

Title: Registry-Free Process Scope COR_PROFILER
- description: Adversaries may leverage the COR_PROFILER environment variable to hijack the execution flow of programs that lo

The COR_PROFILER is a .NET Framework feature which allows developers to specify an unmanaged (or external of .NET) profiling DLL to be loaded into each .NET process that loads the Common Language Runtime (CLR). These profiliers are designed to monitor, troubleshoot, and debug managed code executed by the .NET CLR. (Citation: Microsoft Profiling Mar 2017) (Citation: Microsoft COR_PROFILER Feb 2013)

- category: data/rules/windows/powershell/powershell_script
- level: medium
- id: 23590215-4702-4a70-8805-8dc9e58314a2

Title: Suspicious PowerShell Invocations - Generic
- description: Detects suspicious PowerShell invocation command parameters
- category: data/rules/windows/powershell/powershell_script
- level: high
- id: ed965133-513f-41d9-a441-e38076a0798f

Title: NTFS Alternate Data Stream
- description: Detects writing data into NTFS alternate data streams from powershell. Needs Script Block Logging.
- category: data/rules/windows/powershell/powershell_script
- level: high
- id: 8c521530-5169-495d-a199-0a3a881ad24e

Title: Suspicious SSL Connection
- description: Adversaries may employ a known encryption algorithm to conceal command and control traffic rather than relying
- category: data/rules/windows/powershell/powershell_script
- level: low
- id: 195626f3-5f1b-4403-93b7-e6cfd4d6a078

Title: PowerShell ADRecon Execution
- description: Detects execution of ADRecon.ps1 for AD reconnaissance which has been reported to be actively used by FIN7
- category: data/rules/windows/powershell/powershell_script
- level: high
- id: bf72941a-cba0-41ea-b18c-9aca3925690d

Title: PowerShell Create Local User
- description: Detects creation of a local user via PowerShell
- category: data/rules/windows/powershell/powershell_script
- level: medium
- id: 243de76f-4725-4f2e-8225-a8a69b15ad61

Title: Powershell Exfiltration Over SMTP
- description: Adversaries may steal data by exfiltrating it over an un-encrypted network protocol other than that of the exis

The data may also be sent to an alternate network location from the main command and control server.

- category: data/rules/windows/powershell/powershell_script
- level: medium
- id: 9a7afa56-4762-43eb-807d-c3dc9ffe211b

Title: Suspicious Unblock-File
- description: Remove the Zone.Identifier alternate data stream which identifies the file as downloaded from the internet.
- category: data/rules/windows/powershell/powershell_script
- level: medium
- id: 5947497f-1aa4-41dd-9693-c9848d58727d

Title: Dnscat Execution
- description: Dnscat exfiltration tool execution
- category: data/rules/windows/powershell/powershell_script
- level: critical
- id: a6d67db4-6220-436d-8afc-f3842fe05d43

Title: PowerShell PSAttack
- description: Detects the use of PSAttack PowerShell hack tool
- category: data/rules/windows/powershell/powershell_script
- level: high
- id: b7ec41a4-042c-4f31-a5db-d0fcde9fa5c5

Title: Host Without Firewall
- description: Host Without Firewall. Alert means not complied. Sigma for Qualys vulnerability scanner. Scan type - Vulnerabil
- category: data/rules/compliance
- level: low
- id: 6b2066c8-3dc7-4db7-9db0-6cc1d7b0dde9

Title: Cleartext Protocol Usage
- description: Ensure that all account usernames and authentication credentials are transmitted across networks using encrypte

- category: data/rules/compliance
- level: low
- id: 7e4bfe58-4a47-4709-828d-d86c78b7cc1f

Title: Cleartext Protocol Usage
- description: Ensure that all account usernames and authentication credentials are transmitted across networks using encrypte
- category: data/rules/compliance
- level: low
- id: d7fb8f0e-bd5f-45c2-b467-19571c490d7e

Title: Default Credentials Usage
- description: Before deploying any new asset, change all default passwords to have values consistent with administrative leve
- category: data/rules/compliance
- level: medium
- id: 1a395cbc-a84a-463a-9086-ed8a70e573c7

Title: Locked Workstation
- description: Automatically lock workstation sessions after a standard period of inactivity. The case is not applicable for U
- category: data/rules/compliance
- level: low
- id: 411742ad-89b0-49cb-a7b0-3971b5c1e0a4

Title: Group Modification Logging
- description: Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned
- category: data/rules/compliance
- level: low
- id: 9cf01b6c-e723-4841-a868-6d7f8245ca6e

Title: Cron Files
- description: Detects creation of cron files or files in Cron directories. Potential persistence.
- category: data/rules/linux/file_create
- level: medium
- id: 6c4e2f43-d94d-4ead-b64d-97e53fa2bd05

Title: Linux Doas Conf File Creation
- description: Detects the creation of doas.conf file in linux host platform.
- category: data/rules/linux/file_create
- level: medium
- id: 00eee2a5-fdb0-4746-a21d-e43fbdea5681

Title: OMIGOD SCX RunAsProvider ExecuteShellCommand
- description: Rule to detect the use of the SCX RunAsProvider Invoke_ExecuteShellCommand to execute any UNIX/Linux command us
- category: data/rules/linux/process_creation
- level: high
- id: 21541900-27a9-4454-9c4c-3f0a4240344a

Title: Commands to Clear or Remove the Syslog
- description: Detects specific commands commonly used to remove or empty the syslog.
- category: data/rules/linux/process_creation
- level: high
- id: 3fcc9b35-39e4-44c0-a2ad-9e82b6902b31

Title: OMIGOD SCX RunAsProvider ExecuteScript
- description: Rule to detect the use of the SCX RunAsProvider ExecuteScript to execute any UNIX/Linux script using the /bin/s
- category: data/rules/linux/process_creation
- level: high
- id: 6eea1bf6-f8d2-488a-a742-e6ef6c1b67db

Title: DD File Overwrite
- description: Detects potential overwriting and deletion of a file using DD.
- category: data/rules/linux/process_creation
- level: low
- id: 2953194b-e33c-4859-b9e8-05948c167447

Title: Interactive Bash Suspicious Children
- description: Detects suspicious interactive bash as a parent to rather uncommon child processes
- category: data/rules/linux/process_creation
- level: medium
- id: ea3ecad2-db86-4a89-ad0b-132a10d2db55

Title: Local System Accounts Discovery
- description: Detects enumeration of local systeam accounts
- category: data/rules/linux/process_creation
- level: low
- id: b45e3d6f-42c6-47d8-a478-df6bd6cf534c

Title: BPFtrace Unsafe Option Usage
- description: Detects the usage of the unsafe bpftrace option
- category: data/rules/linux/process_creation
- level: medium
- id: f8341cb2-ee25-43fa-a975-d8a5a9714b39

Title: System Network Connections Discovery
- description: Detects usage of system utilities to discover system network connections
- category: data/rules/linux/process_creation
- level: low
- id: 4c519226-f0cd-4471-bd2f-6fbb2bb68a79

Title: System Network Discovery - Linux
- description: Detects enumeration of local network configuration
- category: data/rules/linux/process_creation
- level: informational
- id: e7bd1cfa-b446-4c88-8afb-403bcd79e3fa

Title: Linux Network Service Scanning
- description: Detects enumeration of local or remote network services.
- category: data/rules/linux/process_creation
- level: low
- id: 3e102cd9-a70d-4a7a-9508-403963092f31

Title: Install Root Certificate
- description: Detects installed new certificate
- category: data/rules/linux/process_creation
- level: low
- id: 78a80655-a51e-4669-bc6b-e9d206a462ee

Title: Local Groups Discovery
- description: Detects enumeration of local system groups
- category: data/rules/linux/process_creation
- level: low
- id: 676381a6-15ca-4d73-a9c8-6a22e970b90d

Title: Linux Shell Pipe to Shell
- description: Detects suspicious process command line that starts with a shell that executes something and finally gets piped
- category: data/rules/linux/process_creation
- level: medium
- id: 880973f3-9708-491c-a77b-2a35a1921158

Title: System Information Discovery
- description: Detects system information discovery commands
- category: data/rules/linux/process_creation
- level: informational
- id: 42df45e7-e6e9-43b5-8f26-bec5b39cc239

Title: Disabling Security Tools
- description: Detects disabling security tools
- category: data/rules/linux/process_creation
- level: medium
- id: e3a8a052-111f-4606-9aee-f28ebeb76776

Title: Clear Linux Logs
- description: Detects clear logs
- category: data/rules/linux/process_creation
- level: medium
- id: 80915f59-9b56-4616-9de0-fd0dea6c12fe

Title: Scheduled Cron Task/Job
- description: Detects abuse of the cron utility to perform task scheduling for initial or recurring execution of malicious co

- category: data/rules/linux/process_creation
- level: medium
- id: 6b14bac8-3e3a-4324-8109-42f0546a347f

Title: Linux Doas Tool Execution
- description: Detects the doas tool execution in linux host platform.
- category: data/rules/linux/process_creation
- level: low
- id: 067d8238-7127-451c-a9ec-fa78045b618b

Title: File Deletion
- description: Detects file deletion commands
- category: data/rules/linux/process_creation
- level: informational
- id: 30aed7b6-d2c1-4eaf-9382-b6bc43e50c57

Title: Linux Webshell Indicators
- description: Detects suspicious sub processes of web server processes
- category: data/rules/linux/process_creation
- level: critical
- id: 818f7b24-0fba-4c49-a073-8b755573b9c7

Title: File and Directory Discovery
- description: Detects usage of system utilities to discover files and directories
- category: data/rules/linux/process_creation
- level: informational
- id: d3feb4ee-ff1d-4d3d-bd10-5b28a238cc72

Title: Scheduled Task/Job At
- description: Detects the use of at/atd
- category: data/rules/linux/process_creation
- level: low
- id: d2d642d7-b393-43fe-bae4-e81ed5915c4b

Title: Linux Crypto Mining Indicators
- description: Detects command line parameters or strings often used by crypto miners
- category: data/rules/linux/process_creation
- level: high
- id: 9069ea3c-b213-4c52-be13-86506a227ab1

Title: Decode Base64 Encoded Text
- description: Detects usage of base64 utility to decode arbitrary base64-encoded text
- category: data/rules/linux/process_creation
- level: low
- id: e2072cab-8c9a-459b-b63c-40ae79e27031

Title: Clipboard Collection with Xclip Tool
- description: Detects attempts to collect data stored in the clipboard from users with the usage of xclip tool. Xclip has to
- category: data/rules/linux/process_creation
- level: low
- id: ec127035-a636-4b9a-8555-0efd4e59f316

Title: Security Software Discovery
- description: Detects usage of system utilities (only grep for now) to discover security software discovery
- category: data/rules/linux/process_creation
- level: low
- id: c9d8b7fd-78e4-44fe-88f6-599135d46d60

Title: Process Discovery
- description: Detects process discovery commands
- category: data/rules/linux/process_creation
- level: informational
- id: 4e2f5868-08d4-413d-899f-dc2f1508627b

Title: Linux Remote System Discovery
- description: Detects the enumeration of other remote systems.
- category: data/rules/linux/process_creation
- level: low
- id: 11063ec2-de63-4153-935e-b1a8b9e616f1

Title: Multiple Modsecurity Blocks
- description: Detects multiple blocks by the mod_security module (Web Application Firewall)
- category: data/rules/linux/modsecurity
- level: medium
- id: a06eea10-d932-4aa6-8ba9-186df72c8d23

Title: Logging Configuration Changes on Linux Host
- description: Detect changes of syslog daemons configuration files
- category: data/rules/linux/auditd
- level: high
- id: c830f15d-6f6e-430f-8074-6f73d6807841

Title: Masquerading as Linux Crond Process
- description: Masquerading occurs when the name or location of an executable, legitimate or malicious, is manipulated or abus
- category: data/rules/linux/auditd
- level: medium
- id: 9d4548fa-bba0-4e88-bd66-5d5bf516cda0

Title: Steganography Hide Zip Information in Picture File
- description: Detects appending of zip file to image
- category: data/rules/linux/auditd
- level: low
- id: 45810b50-7edc-42ca-813b-bdac02fb946b

Title: Possible Coin Miner CPU Priority Param
- description: Detects command line parameter very often used with coin miners
- category: data/rules/linux/auditd
- level: critical
- id: 071d5e5a-9cef-47ec-bc4e-a42e34d8d0ed

Title: System Information Discovery
- description: Detects System Information Discovery commands
- category: data/rules/linux/auditd
- level: low
- id: f34047d9-20d3-4e8b-8672-0a35cc50dc71

Title: Steganography Hide Files with Steghide
- description: Detects embeding of files with usage of steghide binary, the adversaries may use this technique to prevent the
- category: data/rules/linux/auditd
- level: low
- id: ce446a9e-30b9-4483-8e38-d2c9ad0a2280

Title: Creation Of An User Account
- description: Detects the creation of a new user account. Such accounts may be used for persistence that do not require persi
- category: data/rules/linux/auditd
- level: medium
- id: 759d0d51-bc99-4b5e-9add-8f5b2c8e7512

Title: Edit of .bash_profile and .bashrc
- description: Detects change of user environment. Adversaries can insert code into these files to gain persistence each time
- category: data/rules/linux/auditd
- level: medium
- id: e74e15cc-c4b6-4c80-b7eb-dfe49feb7fe9

Title: Data Exfiltration with Wget
- description: Detects attempts to post the file with the usage of wget utility. The adversary can bypass the permission restr
- category: data/rules/linux/auditd
- level: medium
- id: cb39d16b-b3b6-4a7a-8222-1cf24b686ffc

Title: Loading of Kernel Module via Insmod
- description: Detects loading of kernel modules with insmod command. Loadable Kernel Modules (LKMs) are pieces of code that c
- category: data/rules/linux/auditd
- level: high
- id: 106d7cbd-80ff-4985-b682-a7043e5acb72

Title: Clipboard Collection with Xclip Tool
- description: Detects attempts to collect data stored in the clipboard from users with the usage of xclip tool. Xclip has to

- category: data/rules/linux/auditd
- level: low
- id: 214e7e6c-f21b-47ff-bb6f-551b2d143fcf

Title: System Information Discovery
- description: Detects system information discovery commands
- category: data/rules/linux/auditd
- level: informational
- id: 1f358e2e-cb63-43c3-b575-dfb072a6814f

Title: Overwriting the File with Dev Zero or Null
- description: Detects overwriting (effectively wiping/deleting) of a file.
- category: data/rules/linux/auditd
- level: low
- id: 37222991-11e9-4b6d-8bdf-60fbe48f753e

Title: Password Policy Discovery
- description: Detects password policy discovery commands
- category: data/rules/linux/auditd
- level: low
- id: ca94a6db-8106-4737-9ed2-3e3bb826af0a

Title: CVE-2021-3156 Exploitation Attempt
- description: Detects exploitation attempt of vulnerability described in CVE-2021-3156. | Alternative approach might be to lo
- category: data/rules/linux/auditd
- level: critical
- id: 5ee37487-4eb8-4ac2-9be1-d7d14cdc559f

Title: Linux Network Service Scanning
- description: Detects enumeration of local or remote network services.
- category: data/rules/linux/auditd
- level: low
- id: 3761e026-f259-44e6-8826-719ed8079408

Title: Network Sniffing
- description: Network sniffing refers to using the network interface on a system to monitor or capture information sent over
- category: data/rules/linux/auditd
- level: low
- id: f4d3748a-65d1-4806-bd23-e25728081d01

Title: Split A File Into Pieces
- description: Detection use of the command "split" to split files into parts and possible transfer.
- category: data/rules/linux/auditd
- level: low
- id: 2dad0cba-c62a-4a4f-949f-5f6ecd619769

Title: CVE-2021-3156 Exploitation Attempt
- description: Detects exploitation attempt of vulnerability described in CVE-2021-3156. | Alternative approach might be to lo
- category: data/rules/linux/auditd
- level: critical
- id: b9748c98-9ea7-4fdb-80b6-29bed6ba71d2

Title: System Owner or User Discovery
- description: Adversaries may use the information from System Owner/User Discovery during automated discovery to shape follow
- category: data/rules/linux/auditd
- level: low
- id: 9a0d8ca0-2385-4020-b6c6-cb6153ca56f3

Title: Auditing Configuration Changes on Linux Host
- description: Detect changes in auditd configuration files
- category: data/rules/linux/auditd
- level: high
- id: 977ef627-4539-4875-adf4-ed8f780c4922

Title: Hidden Files and Directoriese
- description: Detects adversary creating hidden file or directory, by detecting directories or files with . as the first char
- category: data/rules/linux/auditd
- level: low
- id: d08722cd-3d09-449a-80b4-83ea2d9d4616

Title: Systemd Service Reload or Start
- description: Detects a reload or a start of a service.
- category: data/rules/linux/auditd
- level: low
- id: 2625cc59-0634-40d0-821e-cb67382a3dd7

Title: System Shutdown/Reboot
- description: Adversaries may shutdown/reboot systems to interrupt access to, or aid in the destruction of, those systems.
- category: data/rules/linux/auditd
- level: informational
- id: 4cb57c2f-1f29-41f8-893d-8bed8e1c1d2f

Title: Clipboard Collection of Image Data with Xclip Tool
- description: Detects attempts to collect image data stored in the clipboard from users with the usage of xclip tool. Xclip h
- category: data/rules/linux/auditd
- level: low
- id: f200dc3f-b219-425d-a17e-c38467364816

Title: Binary Padding
- description: Adversaries may use binary padding to add junk data and change the on-disk representation of malware. This rule
- category: data/rules/linux/auditd
- level: high
- id: c52a914f-3d8b-4b2a-bb75-b3991e75f8ba

Title: Remove Immutable File Attribute
- description: Detects removing immutable file attribute.
- category: data/rules/linux/auditd
- level: medium
- id: a5b977d6-8a81-4475-91b9-49dbfcd941f7

Title: File Time Attribute Change
- description: Detect file time attribute change to hide new or changes to existing files.
- category: data/rules/linux/auditd
- level: medium
- id: b3cec4e7-6901-4b0d-a02d-8ab2d8eb818b

Title: Steganography Extract Files with Steghide
- description: Detects extraction of files with usage of steghide binary, the adversaries may use this technique to prevent th
- category: data/rules/linux/auditd
- level: low
- id: a5a827d9-1bbe-4952-9293-c59d897eb41b

Title: Suspicious Commands Linux
- description: Detects relevant commands often related to malware or hacking activity
- category: data/rules/linux/auditd
- level: medium
- id: 1543ae20-cbdf-4ec1-8d12-7664d667a825

Title: Audio Capture
- description: Detects attempts to record audio with arecord utility
- category: data/rules/linux/auditd
- level: low
- id: a7af2487-9c2f-42e4-9bb9-ff961f0561d5

Title: File or Folder Permissions Change
- description: Detects file and folder permission changes.
- category: data/rules/linux/auditd
- level: low
- id: 74c01ace-0152-4094-8ae2-6fd776dd43e5

Title: Disable System Firewall
- description: Detects disabling of system firewalls which could be used by adversaries to bypass controls that limit usage of
- category: data/rules/linux/auditd
- level: high
- id: 53059bc0-1472-438b-956a-7508a94a91f0

Title: Program Executions in Suspicious Folders
- description: Detects program executions in suspicious non-program folders related to malware or hacking activity

- category: data/rules/linux/auditd
- level: medium
- id: a39d7fa7-3fbd-4dc2-97e1-d87f546b1bbc

Title: Linux Capabilities Discovery
- description: Detects attempts to discover the files with setuid/setgid capabilitiy on them. That would allow adversary to es
- category: data/rules/linux/auditd
- level: low
- id: fe10751f-1995-40a5-aaa2-c97ccb4123fe

Title: CVE-2021-4034 Exploitation Attempt
- description: Detects exploitation attempt of vulnerability described in CVE-2021-4034.
- category: data/rules/linux/auditd
- level: high
- id: 40a016ab-4f48-4eee-adde-bbf612695c53

Title: Steganography Unzip Hidden Information From Picture File
- description: Detects extracting of zip file from image file
- category: data/rules/linux/auditd
- level: low
- id: edd595d7-7895-4fa7-acb3-85a18a8772ca

Title: Webshell Remote Command Execution
- description: Detects possible command execution by web application/web shell
- category: data/rules/linux/auditd
- level: critical
- id: c0d3734d-330f-4a03-aae2-65dacc6a8222

Title: Suspicious C2 Activities
- description: Detects suspicious activities as declared by Florian Roth in its 'Best Practice Auditd Configuration'. This inc
- category: data/rules/linux/auditd
- level: medium
- id: f7158a64-6204-4d6d-868a-6e6378b467e0

Title: Modification of ld.so.preload
- description: Identifies modification of ld.so.preload for shared object injection. This technique is used by attackers to lo
- category: data/rules/linux/auditd
- level: high
- id: 4b3cb710-5e83-4715-8c45-8b2b5b3e5751

Title: Screen Capture with Import Tool
- description: Detects adversary creating screen capture of a desktop with Import Tool. Highly recommended using rule on serve
- category: data/rules/linux/auditd
- level: low
- id: dbe4b9c5-c254-4258-9688-d6af0b7967fd

Title: OMIGOD SCX RunAsProvider ExecuteShellCommand
- description: Rule to detect the use of the SCX RunAsProvider Invoke_ExecuteShellCommand to execute any UNIX/Linux command us
- category: data/rules/linux/auditd
- level: high
- id: 045b5f9c-49f7-4419-a236-9854fb3c827a

Title: Data Compressed
- description: An adversary may compress data (e.g., sensitive documents) that is collected prior to exfiltration in order to
- category: data/rules/linux/auditd
- level: low
- id: a3b5e3e9-1b49-4119-8b8e-0344a01f21ee

Title: Suspicious History File Operations
- description: Detects commandline operations on shell history files
- category: data/rules/linux/auditd
- level: medium
- id: eae8ce9f-bde9-47a6-8e79-f20d18419910

Title: Credentials In Files
- description: Detecting attempts to extract passwords with grep
- category: data/rules/linux/auditd
- level: high
- id: df3fcaea-2715-4214-99c5-0056ea59eb35

Title: Screen Capture with Xwd
- description: Detects adversary creating screen capture of a full with xwd. Highly recommended using rule on servers, due hig
- category: data/rules/linux/auditd
- level: low
- id: e2f17c5d-b02a-442b-9052-6eb89c9fec9c

Title: Systemd Service Creation
- description: Detects a creation of systemd services which could be used by adversaries to execute malicious code.
- category: data/rules/linux/auditd
- level: medium
- id: 1bac86ba-41aa-4f62-9d6b-405eac99b485

Title: Clear Command History
- description: Clear command history in linux which is used for defense evasion.
- category: data/rules/linux/builtin
- level: high
- id: fdc88d25-96fb-4b7c-9633-c0e417fdbd4e

Title: Suspicious Log Entries
- description: Detects suspicious log entries in Linux log files
- category: data/rules/linux/builtin
- level: medium
- id: f64b6e9a-5d9d-48a5-8289-e1dd2b3876e1

Title: Space After Filename
- description: Detects space after filename
- category: data/rules/linux/builtin
- level: low
- id: 879c3015-c88b-4782-93d7-07adf92dbcb7

Title: Symlink Etc Passwd
- description: Detects suspicious command lines that look as if they would create symbolic links to /etc/passwd
- category: data/rules/linux/builtin
- level: high
- id: c67fc22a-0be5-4b4f-aad5-2b32c4b69523

Title: Sudo Privilege Escalation CVE-2019-14287
- description: Detects users trying to exploit sudo vulnerability reported in CVE-2019-14287
- category: data/rules/linux/builtin
- level: critical
- id: f74107df-b6c6-4e80-bf00-4170b658162b

Title: Equation Group Indicators
- description: Detects suspicious shell commands used in various Equation Group scripts and tools
- category: data/rules/linux/builtin
- level: high
- id: 41e5c73d-9983-4b69-bd03-e13b67e9623c

Title: Shellshock Expression
- description: Detects shellshock expressions in log files
- category: data/rules/linux/builtin
- level: high
- id: c67e0c98-4d39-46ee-8f6b-437ebf6b950e

Title: Remote File Copy
- description: Detects the use of tools that copy files from or to remote systems
- category: data/rules/linux/builtin
- level: low
- id: 7a14080d-a048-4de8-ae58-604ce58a795b

Title: Code Injection by ld.so Preload
- description: Detects the ld.so preload persistence file. See `man ld.so` for more information.
- category: data/rules/linux/builtin
- level: high
- id: 7e3c4651-c347-40c4-b1d4-d48590fdf684

Title: JexBoss Command Sequence
- description: Detects suspicious command sequence that JexBoss

- category: data/rules/linux/builtin
- level: high
- id: 8ec2c8b4-557a-4121-b87c-5dfb3a602fae

Title: Nimbuspwn Exploitation
- description: Detects exploitation of Nimbuspwn privilege escalation vulnerability (CVE-2022-29799 and CVE-2022-29800)
- category: data/rules/linux/builtin
- level: high
- id: 7ba05b43-adad-4c02-b5e9-c8c35cdf9fa8

Title: Sudo Privilege Escalation CVE-2019-14287
- description: Detects users trying to exploit sudo vulnerability reported in CVE-2019-14287
- category: data/rules/linux/builtin
- level: critical
- id: 7fcc54cb-f27d-4684-84b7-436af096f858

Title: Buffer Overflow Attempts
- description: Detects buffer overflow attempts in Unix system log files
- category: data/rules/linux/builtin
- level: high
- id: 18b042f0-2ecd-4b6e-9f8d-aa7a7e7de781

Title: Setuid and Setgid
- description: Detects suspicious change of file privileges with chown and chmod commands
- category: data/rules/linux/builtin
- level: low
- id: c21c4eaa-ba2e-419a-92b2-8371703cbe21

Title: Modifying Crontab
- description: Detects suspicious modification of crontab file.
- category: data/rules/linux/builtin
- level: medium
- id: af202fd3-7bff-4212-a25a-fb34606cfcbe

Title: Connection Proxy
- description: Detects setting proxy
- category: data/rules/linux/builtin
- level: low
- id: 72f4ab3f-787d-495d-a55d-68c2ff46cf4c

Title: Suspicious Use of /dev/tcp
- description: Detects suspicious command with /dev/tcp
- category: data/rules/linux/builtin
- level: medium
- id: 6cc5fceb-9a71-4c23-aeeb-963abe0b279c

Title: Suspicious Activity in Shell Commands
- description: Detects suspicious shell commands used in various exploit codes (see references)
- category: data/rules/linux/builtin
- level: high
- id: 2aa1440c-9ae9-4d92-84a7-a9e5f5e31695

Title: Privilege Escalation Preparation
- description: Detects suspicious shell commands indicating the information gathering phase as preparation for the Privilege E
- category: data/rules/linux/builtin
- level: medium
- id: 444ade84-c362-4260-b1f3-e45e20e1a905

Title: PwnKit Local Privilege Escalation
- description: Detects potential PwnKit exploitation CVE-2021-4034 in auth logs
- category: data/rules/linux/builtin
- level: high
- id: 0506a799-698b-43b4-85a1-ac4c84c720e9

Title: Commands to Clear or Remove the Syslog
- description: Detects specific commands commonly used to remove or empty the syslog
- category: data/rules/linux/builtin
- level: high
- id: e09eb557-96d2-4de9-ba2d-30f712a5afd3

Title: Suspicious Reverse Shell Command Line
- description: Detects suspicious shell commands or program code that may be executed or used in command line to establish a r
- category: data/rules/linux/builtin
- level: high
- id: 738d9bcf-6999-4fdb-b4ac-3033037db8ab

Title: Linux Crypto Mining Pool Connections
- description: Detects process connections to a Monero crypto mining pool
- category: data/rules/linux/network_connection
- level: high
- id: a46c93b7-55ed-4d27-a41b-c259456c4746

Title: Linux Reverse Shell Indicator
- description: Detects a bash contecting to a remote IP address (often found when actors do something like 'bash -i >& /dev/tc
- category: data/rules/linux/network_connection
- level: critical
- id: 83dcd9f6-9ca8-4af7-a16e-a1c7a6b51871

Title: Guacamole Two Users Sharing Session Anomaly
- description: Detects suspicious session with two users present
- category: data/rules/linux/other
- level: high
- id: 1edd77db-0669-4fef-9598-165bda82826d

Title: Suspicious OpenSSH Daemon Error
- description: Detects suspicious SSH / SSHD error messages that indicate a fatal or suspicious error that could be caused by
- category: data/rules/linux/other
- level: medium
- id: e76b413a-83d0-4b94-8e4c-85db4a5b8bdc

Title: Disabling Security Tools
- description: Detects disabling security tools
- category: data/rules/linux/other
- level: medium
- id: 49f5dfc1-f92e-4d34-96fa-feba3f6acf36

Title: Relevant ClamAV Message
- description: Detects relevant ClamAV messages
- category: data/rules/linux/other
- level: high
- id: 36aa86ca-fd9d-4456-814e-d3b1b8e1e0bb

Title: SSHD Error Message CVE-2018-15473
- description: Detects exploitation attempt using public exploit code for CVE-2018-15473
- category: data/rules/linux/other
- level: medium
- id: 4c9d903d-4939-4094-ade0-3cb748f4d7da

Title: Suspicious Named Error
- description: Detects suspicious DNS error messages that indicate a fatal or suspicious error that could be caused by exploit
- category: data/rules/linux/other
- level: high
- id: c8e35e96-19ce-4f16-aeb6-fd5588dc5365

Title: Failed Logins with Different Accounts from Single Source System
- description: Detects suspicious failed logins with different user accounts from a single source system
- category: data/rules/linux/other
- level: medium
- id: fc947f8e-ea81-4b14-9a7b-13f888f94e18

Title: Suspicious VSFTPD Error Messages
- description: Detects suspicious VSFTPD error messages that indicate a fatal or suspicious error that could be caused by expl
- category: data/rules/linux/other
- level: medium
- id: 377f33a1-4b36-4ee1-acee-1dbe4b43cfbe

Title: Possible DNS Tunneling
- description: Normally, DNS logs contain a limited amount of different dns queries for a single domain. This rule detects a h

- category: data/rules/network
- level: high
- id: 1ec4b281-aa65-46a2-bdae-5fd830ed914e

Title: High DNS Requests Rate
- description: High DNS requests amount from host per short period of time
- category: data/rules/network
- level: medium
- id: 51186749-7415-46be-90e5-6914865c825a

Title: Telegram Bot API Request
- description: Detects suspicious DNS queries to api.telegram.org used by Telegram Bots of any kind
- category: data/rules/network
- level: medium
- id: c64c5175-5189-431b-a55e-6d9882158251

Title: High TXT Records Requests Rate
- description: Extremely high rate of TXT record type DNS requests from host per short period of time. Possible result of Do-e
- category: data/rules/network
- level: medium
- id: f0a8cedc-1d22-4453-9c44-8d9f4ebd5d35

Title: DNS TXT Answer with Possible Execution Strings
- description: Detects strings used in command execution in DNS TXT Answer
- category: data/rules/network
- level: high
- id: 8ae51330-899c-4641-8125-e39f2e07da72

Title: Network Scans Count By Destination IP
- description: Detects many failed connection attempts to different ports or hosts
- category: data/rules/network
- level: medium
- id: 4601eaec-6b45-4052-ad32-2d96d26ce0d8

Title: Cobalt Strike DNS Beaconing
- description: Detects suspicious DNS queries known from Cobalt Strike beacons
- category: data/rules/network
- level: critical
- id: 2975af79-28c4-4d2f-a951-9095f229df29

Title: High DNS Requests Rate
- description: High DNS requests amount from host per short period of time
- category: data/rules/network
- level: medium
- id: b4163085-4001-46a3-a79a-55d8bbbc7a3a

Title: Suspicious DNS Query with B64 Encoded String
- description: Detects suspicious DNS queries using base64 encoding
- category: data/rules/network
- level: medium
- id: 4153a907-2451-4e4f-a578-c52bb6881432

Title: Equation Group C2 Communication
- description: Detects communication to C2 servers mentioned in the operational notes of the ShadowBroker leak of EquationGrou
- category: data/rules/network
- level: high
- id: 881834a4-6659-4773-821e-1c151789d873

Title: High DNS Bytes Out
- description: High DNS queries bytes amount from host per short period of time
- category: data/rules/network
- level: medium
- id: 0f6c1bf5-70a5-4963-aef9-aab1eefb50bd

Title: Monero Crypto Coin Mining Pool Lookup
- description: Detects suspicious DNS queries to Monero mining pools
- category: data/rules/network
- level: high
- id: b593fd50-7335-4682-a36c-4edcb68e4641

Title: High NULL Records Requests Rate
- description: Extremely high rate of NULL record type DNS requests from host per short period of time. Possible result of iod
- category: data/rules/network
- level: medium
- id: 44ae5117-9c44-40cf-9c7c-7edad385ca70

Title: Network Scans Count By Destination Port
- description: Detects many failed connection attempts to different ports or hosts
- category: data/rules/network
- level: medium
- id: fab0ddf0-b8a9-4d70-91ce-a20547209afb

Title: High DNS Bytes Out
- description: High DNS queries bytes amount from host per short period of time
- category: data/rules/network
- level: medium
- id: 3b6e327d-8649-4102-993f-d25786481589

Title: Wannacry Killswitch Domain
- description: Detects wannacry killswitch domain dns queries
- category: data/rules/network
- level: high
- id: 3eaf6218-3bed-4d8a-8707-274096f12a18

Title: Possible PrintNightmare Print Driver Install
- description: Detects the remote installation of a print driver which is possible indication of the exploitation of PrintNigh

The occurrence of print drivers being installed remotely via RPC functions should be rare, as print drivers are normally installed locally and or through group policy.

- category: data/rules/network/zeek
- level: medium
- id: 7b33baef-2a75-4ca3-9da4-34f9a15382d8

Title: New Kind of Network (NKN) Detection
- description: NKN is a networking service using blockchain technology to support a decentralized network of peers. While ther
- category: data/rules/network/zeek
- level: low
- id: fa7703d6-0ee8-4949-889c-48c84bc15b6f

Title: SMB Spoolss Name Piped Usage
- description: Detects the use of the spoolss named pipe over SMB. This can be used to trigger the authentication via NTLM of
- category: data/rules/network/zeek
- level: medium
- id: bae2865c-5565-470d-b505-9496c87d0c30

Title: Suspicious Access to Sensitive File Extensions - Zeek
- description: Detects known sensitive file extensions via Zeek
- category: data/rules/network/zeek
- level: medium
- id: 286b47ed-f6fe-40b3-b3a8-35129acd43bc

Title: Default Cobalt Strike Certificate
- description: Detects the presence of default Cobalt Strike certificate in the HTTPS traffic
- category: data/rules/network/zeek
- level: high
- id: 7100f7e3-92ce-4584-b7b7-01b40d3d4118

Title: DNS Events Related To Mining Pools
- description: Identifies clients that may be performing DNS lookups associated with common currency mining pools.
- category: data/rules/network/zeek
- level: low
- id: bf74135c-18e8-4a72-a926-0e4f47888c19

Title: Suspicious PsExec Execution - Zeek
- description: detects execution of psexec or paexec with renamed service name, this rule helps to filter out the noise if pse
- category: data/rules/network/zeek
- level: high

- id: f1b3a22a-45e6-4004-afb5-4291f9c21166

Title: Kerberos Network Traffic RC4 Ticket Encryption
- description: Detects kerberos TGS request using RC4 encryption which may be indicative of kerberoasting
- category: data/rules/network/zeek
- level: medium
- id: 503fe26e-b5f2-4944-a126-eab405cc06e5

Title: MITRE BZAR Indicators for Execution
- description: Windows DCE-RPC functions which indicate an execution techniques on the remote system. All credit for the Zeek
- category: data/rules/network/zeek
- level: medium
- id: b640c0b8-87f8-4daa-aef8-95a24261dd1d

Title: WebDav Put Request
- description: A General detection for WebDav user-agent being used to PUT files on a WebDav network share. This could be an i
- category: data/rules/network/zeek
- level: low
- id: 705072a5-bb6f-4ced-95b6-ecfa6602090b

Title: Domain User Enumeration Network Recon 01
- description: Domain user and group enumeration via network reconnaissance. Seen in APT 29 and other common tactics and actor
- category: data/rules/network/zeek
- level: medium
- id: 66a0bdc6-ee04-441a-9125-99d2eb547942

Title: Publicly Accessible RDP Service
- description: Detects connections from routable IPs to an RDP listener - which is indicative of a publicly-accessible RDP ser
- category: data/rules/network/zeek
- level: high
- id: 1fc0809e-06bf-4de3-ad52-25e5263b7623

Title: First Time Seen Remote Named Pipe - Zeek
- description: This detection excludes known namped pipes accessible remotely and notify on newly observed ones, may help to d
- category: data/rules/network/zeek
- level: high
- id: 021310d9-30a6-480a-84b7-eaa69aeb92bb

Title: Possible Impacket SecretDump Remote Activity - Zeek
- description: Detect AD credential dumping using impacket secretdump HKTL. Based on the SIGMA rules/windows/builtin/win_impac
- category: data/rules/network/zeek
- level: high
- id: 92dae1ed-1c9d-4eff-a567-33acbd95b00e

Title: OMIGOD HTTP No Authentication RCE
- description: Detects the exploitation of OMIGOD (CVE-2021-38647) which allows remote execute (RCE) commands as root with jus
- category: data/rules/network/zeek
- level: high
- id: ab6b1a39-a9ee-4ab4-b075-e83acf6e346b

Title: Remote Task Creation via ATSVC Named Pipe - Zeek
- description: Detects remote task creation via at.exe or API interacting with ATSVC namedpipe
- category: data/rules/network/zeek
- level: medium
- id: dde85b37-40cd-4a94-b00c-0b8794f956b5

Title: MITRE BZAR Indicators for Persistence
- description: Windows DCE-RPC functions which indicate a persistence techniques on the remote system. All credit for the Zeek
- category: data/rules/network/zeek
- level: medium
- id: 53389db6-ba46-48e3-a94c-e0f2cefe1583

Title: Executable from Webdav
- description: Detects executable access via webdav6. Can be seen in APT 29 such as from the emulated APT 29 hackathon https:/
- category: data/rules/network/zeek
- level: medium
- id: aac2fd97-bcba-491b-ad66-a6edf89c71bf

Title: Suspicious DNS Z Flag Bit Set

- description: The DNS Z flag is bit within the DNS protocol header that is, per the IETF design, meant to be used reserved (u
- category: data/rules/network/zeek
- level: medium
- id: ede05abc-2c9e-4624-9944-9ff17fdc0bf5

Title: Potential PetitPotam Attack Via EFS RPC Calls
- description: Detects usage of the windows RPC library Encrypting File System Remote Protocol (MS-EFSRPC). Variations of this

The usage of this RPC function should be rare if ever used at all. Thus usage of this function is uncommon enough that any usage of this RPC function should warrant further investigation to determine if it is legitimate. View surrounding logs (within a few minutes before and after) from the Source IP to. Logs from from the Source IP would include dce_rpc, smb_mapping, smb_files, rdp, ntlm, kerberos, etc..'

- category: data/rules/network/zeek
- level: medium
- id: 4096842a-8f9f-4d36-92b4-d0b2a62f9b2a

Title: Transferring Files with Credential Data via Network Shares - Zeek
- description: Transferring files with well-known filenames (sensitive files with credential data) using network shares
- category: data/rules/network/zeek
- level: medium
- id: 2e69f167-47b5-4ae7-a390-47764529eff5

Title: DNS TOR Proxies
- description: Identifies IPs performing DNS lookups associated with common Tor proxies.
- category: data/rules/network/zeek
- level: medium
- id: a8322756-015c-42e7-afb1-436e85ed3ff5

Title: Cisco Denial of Service
- description: Detect a system being shutdown or put into different boot mode
- category: data/rules/network/cisco/aaa
- level: medium
- id: d94a35f0-7a29-45f6-90a0-80df6159967c

Title: Cisco Modify Configuration
- description: Modifications to a config that will serve an adversary's impacts or persistence
- category: data/rules/network/cisco/aaa
- level: medium
- id: 671ffc77-50a7-464f-9e3d-9ea2b493b26b

Title: Cisco Disabling Logging
- description: Turn off logging locally or remote
- category: data/rules/network/cisco/aaa
- level: high
- id: 9e8f6035-88bf-4a63-96b6-b17c0508257e

Title: Cisco File Deletion
- description: See what files are being deleted from flash file systems
- category: data/rules/network/cisco/aaa
- level: medium
- id: 71d65515-c436-43c0-841b-236b1f32c21e

Title: Cisco Clear Logs
- description: Clear command history in network OS which is used for defense evasion
- category: data/rules/network/cisco/aaa
- level: high
- id: ceb407f6-8277-439b-951f-e4210e3ed956

Title: Cisco Stage Data
- description: Various protocols maybe used to put data on the device for exfil or infil
- category: data/rules/network/cisco/aaa
- level: low
- id: 5e51acb2-bcbe-435b-99c6-0e3cd5e2aa59

Title: Cisco Sniffing
- description: Show when a monitor or a span/rspan is setup or modified
- category: data/rules/network/cisco/aaa
- level: medium
- id: b9e1f193-d236-4451-aaae-2f3d2102120d

Title: Cisco Collect Data
- description: Collect pertinent data from the configuration files
- category: data/rules/network/cisco/aaa
- level: low
- id: cd072b25-a418-4f98-8ebc-5093fb38fe1a

Title: Cisco Show Commands Input
- description: See what commands are being input into the device by other people, full credentials can be in the history
- category: data/rules/network/cisco/aaa
- level: medium
- id: b094d9fb-b1ad-4650-9f1a-fb7be9f1d34b

Title: Cisco Crypto Commands
- description: Show when private keys are being exported from the device, or when new certificates are installed
- category: data/rules/network/cisco/aaa
- level: high
- id: 1f978c6a-4415-47fb-aca5-736a44d7ca3d

Title: Cisco Discovery
- description: Find information about network devices that is not stored in config files
- category: data/rules/network/cisco/aaa
- level: low
- id: 9705a6a1-6db6-4a16-a987-15b7151e299b

Title: Cisco Local Accounts
- description: Find local accounts being created or modified as well as remote authentication configurations
- category: data/rules/network/cisco/aaa
- level: high
- id: 6d844f0f-1c18-41af-8f19-33e7654edfc3

Title: Django Framework Exceptions
- description: Detects suspicious Django web application framework exceptions that could indicate exploitation attempts
- category: data/rules/application/django
- level: medium
- id: fd435618-981e-4a7c-81f8-f78ce480d616

Title: Spring Framework Exceptions
- description: Detects suspicious Spring framework exceptions that could indicate exploitation attempts
- category: data/rules/application/spring
- level: medium
- id: ae48ab93-45f7-4051-9dfe-5d30a3f78e33

Title: Antivirus Password Dumper Detection
- description: Detects a highly relevant Antivirus alert that reports a password dumper
- category: data/rules/application/antivirus
- level: critical
- id: 78cc2dd2-7d20-4d32-93ff-057084c38b93

Title: Antivirus Hacktool Detection
- description: Detects a highly relevant Antivirus alert that reports a hack tool or other attack tool
- category: data/rules/application/antivirus
- level: high
- id: fa0c05b6-8ad3-468d-8231-c1cbccb64fba

Title: Antivirus Ransomware Detection
- description: Detects a highly relevant Antivirus alert that reports ransomware
- category: data/rules/application/antivirus
- level: critical
- id: 4c6ca276-d4d0-4a8c-9e4c-d69832f8671f

Title: Antivirus Exploitation Framework Detection
- description: Detects a highly relevant Antivirus alert that reports an exploitation framework
- category: data/rules/application/antivirus
- level: critical
- id: 238527ad-3c2c-4e4f-a1f6-92fd63adb864

Title: Antivirus Web Shell Detection
- description: Detects a highly relevant Antivirus alert that reports a web shell. It's highly recommended to tune this rule t

- category: data/rules/application/antivirus
- level: critical
- id: fdf135a2-9241-4f96-a114-bb404948f736

Title: Antivirus PrinterNightmare CVE-2021-34527 Exploit Detection
- description: Detects the suspicious file that is created from PoC code against Windows Print Spooler Remote Code Execution v
- category: data/rules/application/antivirus
- level: critical
- id: 6fe1719e-ecdf-4caf-bffe-4f501cb0a561

Title: Antivirus Relevant File Paths Alerts
- description: Detects an Antivirus alert in a highly relevant file path or with a relevant file name
- category: data/rules/application/antivirus
- level: high
- id: c9a88268-0047-4824-ba6e-4d81ce0b907c

Title: Suspicious SQL Error Messages
- description: Detects SQL error messages that indicate probing for an injection attack
- category: data/rules/application/sql
- level: high
- id: 8a670c6d-7189-4b1c-8017-a417ca84a086

Title: Ruby on Rails Framework Exceptions
- description: Detects suspicious Ruby on Rails exceptions that could indicate exploitation attempts
- category: data/rules/application/ruby
- level: medium
- id: 0d2c3d4c-4b48-4ac3-8f23-ea845746bb1a

Title: Python SQL Exceptions
- description: Generic rule for SQL exceptions in Python according to PEP 249
- category: data/rules/application/python
- level: medium
- id: 19aefed0-ffd4-47dc-a7fc-f8b1425e84f9

Title: Remote Encrypting File System Abuse
- description: Detects remote RPC calls to possibly abuse remote encryption service via MS-EFSR
- category: data/rules/application/rpc_firewall
- level: high
- id: 5f92fff9-82e2-48eb-8fc1-8b133556a551

Title: Remote Event Log Recon
- description: Detects remote RPC calls to get event log information via EVEN or EVEN6
- category: data/rules/application/rpc_firewall
- level: high
- id: 2053961f-44c7-4a64-b62d-f6e72800af0d

Title: Remote Schedule Task Lateral Movement via ATSvc
- description: Detects remote RPC calls to create or execute a scheduled task via ATSvc
- category: data/rules/application/rpc_firewall
- level: high
- id: 0fcd1c79-4eeb-4746-aba9-1b458f7a79cb

Title: Remote DCOM/WMI Lateral Movement
- description: Detects remote RPC calls that performs remote DCOM operations. These could be abused for lateral movement via D
- category: data/rules/application/rpc_firewall
- level: high
- id: 68050b10-e477-4377-a99b-3721b422d6ef

Title: Remote Registry Recon
- description: Detects remote RPC calls to collect information
- category: data/rules/application/rpc_firewall
- level: high
- id: d8ffe17e-04be-4886-beb9-c1dd1944b9a8

Title: SharpHound Recon Account Discovery
- description: Detects remote RPC calls useb by SharpHound to map remote connections and local group membership.
- category: data/rules/application/rpc_firewall
- level: high
- id: 65f77b1e-8e79-45bf-bb67-5988a8ce45a5

Title: SharpHound Recon Sessions
- description: Detects remote RPC calls useb by SharpHound to map remote connections and local group membership.
- category: data/rules/application/rpc_firewall
- level: high
- id: 6d580420-ff3f-4e0e-b6b0-41b90c787e28

Title: Remote Schedule Task Recon via AtScv
- description: Detects remote RPC calls to read information about scheduled tasks via AtScv
- category: data/rules/application/rpc_firewall
- level: high
- id: f177f2bc-5f3e-4453-b599-57eefce9a59c

Title: Remote Registry Lateral Movement
- description: Detects remote RPC calls to modify the registry and possible execute code
- category: data/rules/application/rpc_firewall
- level: high
- id: 35c55673-84ca-4e99-8d09-e334f3c29539

Title: Remote Server Service Abuse for Lateral Movement
- description: Detects remote RPC calls to possibly abuse remote encryption service via MS-EFSR
- category: data/rules/application/rpc_firewall
- level: high
- id: 10018e73-06ec-46ec-8107-9172f1e04ff2

Title: Remote Schedule Task Recon via ITaskSchedulerService
- description: Detects remote RPC calls to read information about scheduled tasks
- category: data/rules/application/rpc_firewall
- level: high
- id: 7f7c49eb-2977-4ac8-8ab0-ab1bae14730e

Title: Remote Printing Abuse for Lateral Movement
- description: Detects remote RPC calls to possibly abuse remote printing service via MS-RPRN / MS-PAR
- category: data/rules/application/rpc_firewall
- level: high
- id: bc3a4b0c-e167-48e1-aa88-b3020950e560

Title: Possible DCSync Attack
- description: Detects remote RPC calls to MS-DRSR from non DC hosts, which could indicate DCSync / DCShadow attacks.
- category: data/rules/application/rpc_firewall
- level: high
- id: 56fda488-113e-4ce9-8076-afc2457922c3

Title: Remote Schedule Task Lateral Movement via SASec
- description: Detects remote RPC calls to read information about scheduled tasks via SASec
- category: data/rules/application/rpc_firewall
- level: high
- id: 0a3ff354-93fc-4273-8a03-1078782de5b7

Title: Remote Server Service Abuse
- description: Detects remote RPC calls to possibly abuse remote encryption service via MS-SRVS
- category: data/rules/application/rpc_firewall
- level: high
- id: b6ea3cc7-542f-43ef-bbe4-980fbed444c7

Title: Remote Schedule Task Lateral Movement via ITaskSchedulerService
- description: Detects remote RPC calls to create or execute a scheduled task
- category: data/rules/application/rpc_firewall
- level: high
- id: ace3ff54-e7fd-46bd-8ea0-74b49a0aca1d

Title: Remote Schedule Task Lateral Movement via SASec
- description: Detects remote RPC calls to create or execute a scheduled task via SASec
- category: data/rules/application/rpc_firewall
- level: high
- id: aff229ab-f8cd-447b-b215-084d11e79eb0

Title: Silence.EDA Detection
- description: Detects Silence empireDNSagent

- category: data/rules/apt
- level: critical
- id: 3ceb2083-a27f-449a-be33-14ec1b7cc973

Title: Silence.Downloader V3
- description: Detects Silence downloader. These commands are hardcoded into the binary.
- category: data/rules/apt
- level: high
- id: 170901d1-de11-4de7-bccb-8fa13678d857

Title: JNDIExploit Pattern
- description: Detects exploitation attempt using the JDNIExploiit Kit
- category: data/rules/web
- level: high
- id: 412d55bc-7737-4d25-9542-5b396867ce55

Title: ADSelfService Exploitation
- description: Detects suspicious access to URLs that was noticed in cases in which attackers exploitated the ADSelfService vu
- category: data/rules/web
- level: high
- id: 6702b13c-e421-44cc-ab33-42cc25570f11

Title: CVE-2020-10148 SolarWinds Orion API Auth Bypass
- description: Detects CVE-2020-10148 SolarWinds Orion API authentication bypass attempts
- category: data/rules/web
- level: critical
- id: 5a35116f-43bc-4901-b62d-ef131f42a9af

Title: VMware vCenter Server File Upload CVE-2021-22005
- description: Detects exploitation attempts using file upload vulnerability CVE-2021-22005 in the VMWare vCenter Server.
- category: data/rules/web
- level: high
- id: b014ea07-8ea0-4859-b517-50a4e5b7ecec

Title: Oracle WebLogic Exploit CVE-2021-2109
- description: Detects the exploitation of the WebLogic server vulnerability described in CVE-2021-2109
- category: data/rules/web
- level: critical
- id: 687f6504-7f44-4549-91fc-f07bab065821

Title: Pulse Secure Attack CVE-2019-11510
- description: Detects CVE-2019-11510 exploitation attempt - URI contains Guacamole
- category: data/rules/web
- level: critical
- id: 2dbc10d7-a797-49a8-8776-49efa6442e60

Title: DEWMODE Webshell Access
- description: Detects access to DEWMODE webshell as described in FIREEYE report
- category: data/rules/web
- level: critical
- id: fdf96c90-42d5-4406-8a9c-14a2c9a016b5

Title: Apache Segmentation Fault
- description: Detects a segmentation fault error message caused by a creashing apache worker process
- category: data/rules/web
- level: high
- id: 1da8ce0b-855d-4004-8860-7d64d42063b1

Title: Grafana Path Traversal Exploitation CVE-2021-43798
- description: Detects a successful Grafana path traversal exploitation
- category: data/rules/web
- level: critical
- id: 7b72b328-5708-414f-9a2a-6a6867c26e16

Title: Apache Threading Error
- description: Detects an issue in apache logs that reports threading related errors
- category: data/rules/web
- level: medium
- id: e9a2b582-3f6a-48ac-b4a1-6849cdc50b3c

Title: Log4j RCE CVE-2021-44228 in Fields
- description: Detects exploitation attempt against log4j RCE vulnerability reported as CVE-2021-44228 in different header fie
- category: data/rules/web
- level: high
- id: 9be472ed-893c-4ec0-94da-312d2765f654

Title: Pulse Connect Secure RCE Attack CVE-2021-22893
- description: This rule detects exploitation attempts using Pulse Connect Secure(PCS) vulnerability (CVE-2021-22893)
- category: data/rules/web
- level: high
- id: 5525edac-f599-4bfd-b926-3fa69860e766

Title: Log4j RCE CVE-2021-44228 Generic
- description: Detects exploitation attempt against log4j RCE vulnerability reported as CVE-2021-44228 (Log4Shell)
- category: data/rules/web
- level: high
- id: 5ea8faa8-db8b-45be-89b0-151b84c82702

Title: ProxyLogon Reset Virtual Directories Based On IIS Log
- description: When exploiting this vulnerability with CVE-2021–26858, an SSRF attack is used to manipulate virtual directorie
- category: data/rules/web
- level: critical
- id: effee1f6-a932-4297-a81f-acb44064fa3a

Title: Fortinet CVE-2021-22123 Exploitation
- description: Detects CVE-2021-22123 exploitation attempt against Fortinet WAFs
- category: data/rules/web
- level: critical
- id: f425637f-891c-4191-a6c4-3bb1b70513b4

Title: Exchange ProxyShell Pattern
- description: Detects URL patterns that could be found in ProxyShell exploitation attempts against Exchange servers (failed a
- category: data/rules/web
- level: medium
- id: 23eee45e-933b-49f9-ae1b-df706d2d52ef

Title: Exchange PowerShell Snap-Ins Used by HAFNIUM
- description: Detects adding and using Exchange PowerShell snap-ins to export mailbox data by HAFNIUM
- category: data/rules/web
- level: high
- id: 25676e10-2121-446e-80a4-71ff8506af47

Title: Oracle WebLogic Exploit
- description: Detects access to a webshell dropped into a keystore folder on the WebLogic server
- category: data/rules/web
- level: critical
- id: 37e8369b-43bb-4bf8-83b6-6dd43bda2000

Title: SonicWall SSL/VPN Jarrewrite Exploit
- description: Detects exploitation attempts of the SonicWall Jarrewrite Exploit
- category: data/rules/web
- level: high
- id: 6f55f047-112b-4101-ad32-43913f52db46

Title: CVE-2021-21978 Exploitation Attempt
- description: Detects the exploitation of the VMware View Planner vulnerability described in CVE-2021-21978
- category: data/rules/web
- level: high
- id: 77586a7f-7ea4-4c41-b19c-820140b84ca9

Title: Oracle WebLogic Exploit CVE-2020-14882
- description: Detects exploitation attempts on WebLogic servers
- category: data/rules/web
- level: high
- id: 85d466b0-d74c-4514-84d3-2bdd3327588b

Title: Successful IIS Shortname Fuzzing Scan
- description: When IIS uses an old .Net Framework it's possible to enumeration folder with the symbol ~.

- category: data/rules/web
- level: medium
- id: 7cb02516-6d95-4ffc-8eee-162075e111ac

Title: Cisco ASA FTD Exploit CVE-2020-3452
- description: Detects exploitation attempts on Cisco ASA FTD systems exploiting CVE-2020-3452 with a status code of 200 (scce
- category: data/rules/web
- level: high
- id: aba47adc-4847-4970-95c1-61dce62a8b29

Title: Confluence Exploitation CVE-2019-3398
- description: Detects the exploitation of the Confluence vulnerability described in CVE-2019-3398
- category: data/rules/web
- level: critical
- id: e9bc39ae-978a-4e49-91ab-5bd481fc668b

Title: Detect XSS Attempts By Keywords
- description: Detects XSS that use GET requests by keyword searches in URL strings
- category: data/rules/web
- level: high
- id: 65354b83-a2ea-4ea6-8414-3ab38be0d409

Title: Detect Sql Injection By Keywords
- description: Detects sql injection that use GET requests by keyword searches in URL strings
- category: data/rules/web
- level: high
- id: 5513deaf-f49a-46c2-a6c8-3f111b5cb453

Title: CVE-2021-21972 VSphere Exploitation
- description: Detects the exploitation of VSphere Remote Code Execution vulnerability as described in CVE-2021-21972
- category: data/rules/web
- level: high
- id: 179ed852-0f9b-4009-93a7-68475910fd86

Title: TerraMaster TOS CVE-2020-28188
- description: Detects the exploitation of the TerraMaster TOS vulnerability described in CVE-2020-28188
- category: data/rules/web
- level: critical
- id: 15c312b9-00d0-4feb-8870-7d940a4bdc5e

Title: Citrix ADS Exploitation CVE-2020-8193 CVE-2020-8195
- description: Detects exploitation attempt against Citrix Netscaler, Application Delivery Controller (ADS) and Citrix Gateway
- category: data/rules/web
- level: critical
- id: 0d0d9a8a-a49e-4e27-b061-7ce4b936cfb7

Title: Exchange Exploitation Used by HAFNIUM
- description: Detects exploitation attempts in Exchange server logs as described in blog posts reporting on HAFNIUM group act
- category: data/rules/web
- level: high
- id: 67bce556-312f-4c81-9162-c3c9ff2599b2

Title: CVE-2021-41773 Exploitation Attempt
- description: Detects exploitation of flaw in path normalization in Apache HTTP server 2.4.49. An attacker could use a path t
- category: data/rules/web
- level: high
- id: 3007fec6-e761-4319-91af-e32e20ac43f5

Title: Arcadyan Router Exploitations
- description: Detects exploitation of vulnerabilities in Arcadyan routers as reported in CVE-2021-20090 and CVE-2021-20091.
- category: data/rules/web
- level: critical
- id: f0500377-bc70-425d-ac8c-e956cd906871

Title: CVE-2021-40539 Zoho ManageEngine ADSelfService Plus Exploit
- description: Detects an authentication bypass vulnerability affecting the REST API URLs in ADSelfService Plus (CVE-2021-4053
- category: data/rules/web
- level: critical
- id: fcbb4a77-f368-4945-b046-4499a1da69d1

Title: Exchange Exploitation CVE-2021-28480
- description: Detects successful exploitation of Exchange vulnerability as reported in CVE-2021-28480
- category: data/rules/web
- level: critical
- id: a2a9d722-0acb-4096-bccc-daaf91a5037b

Title: Source Code Enumeration Detection by Keyword
- description: Detects source code enumeration that use GET requests by keyword searches in URL strings
- category: data/rules/web
- level: medium
- id: 953d460b-f810-420a-97a2-cfca4c98e602

Title: Sitecore Pre-Auth RCE CVE-2021-42237
- description: Detects exploitation attempts of Sitecore Experience Platform Pre-Auth RCE CVE-2021-42237 found in Report.ashx
- category: data/rules/web
- level: high
- id: 20c6ed1c-f7f0-4ea3-aa65-4f198e6acb0f

Title: Path Traversal Exploitation Attempts
- description: Detects path traversal exploitation attempts
- category: data/rules/web
- level: medium
- id: 7745c2ea-24a5-4290-b680-04359cb84b35

Title: Multiple Suspicious Resp Codes Caused by Single Client
- description: Detects possible exploitation activity or bugs in a web application
- category: data/rules/web
- level: medium
- id: 6fdfc796-06b3-46e8-af08-58f3505318af

Title: CVE-2020-5902 F5 BIG-IP Exploitation Attempt
- description: Detects the exploitation attempt of the vulnerability found in F5 BIG-IP and described in CVE-2020-5902
- category: data/rules/web
- level: critical
- id: 44b53b1c-e60f-4a7b-948e-3435a7918478

Title: CVE-2010-5278 Exploitation Attempt
- description: MODx manager - Local File Inclusion:Directory traversal vulnerability in manager/controllers/default/resource/t
- category: data/rules/web
- level: critical
- id: a4a899e8-fd7a-49dd-b5a8-7044def72d61

Title: Webshell ReGeorg Detection Via Web Logs
- description: Certain strings in the uri_query field when combined with null referer and null user agent can indicate activit
- category: data/rules/web
- level: high
- id: 2ea44a60-cfda-11ea-87d0-0242ac130003

Title: CVE-2021-33766 Exchange ProxyToken Exploitation
- description: Detects the exploitation of Microsoft Exchange ProxyToken vulnerability as described in CVE-2021-33766
- category: data/rules/web
- level: critical
- id: 56973b50-3382-4b56-bdf5-f51a3183797a

Title: Webshell Detection by Keyword
- description: Detects webshells that use GET requests by keyword searches in URL strings
- category: data/rules/web
- level: high
- id: 7ff9db12-1b94-4a79-ba68-a2402c5d6729

Title: Exploitation of CVE-2021-26814 in Wazuh
- description: Detects the exploitation of the Wazuh RCE vulnerability described in CVE-2021-26814
- category: data/rules/web
- level: high
- id: b9888738-29ed-4c54-96a4-f38c57b84bb3

Title: CVE-2020-0688 Exploitation Attempt
- description: Detects CVE-2020-0688 Exploitation attempts

- category: data/rules/web
- level: high
- id: 7c64e577-d72e-4c3d-9d75-8de6d1f9146a

Title: Nginx Core Dump
- description: Detects a core dump of a crashing Nginx worker process, which could be a signal of a serious problem or exploit
- category: data/rules/web
- level: high
- id: 59ec40bb-322e-40ab-808d-84fa690d7e56

Title: CVE-2020-0688 Exchange Exploitation via Web Log
- description: Detects the exploitation of Microsoft Exchange vulnerability as described in CVE-2020-0688
- category: data/rules/web
- level: critical
- id: fce2c2e2-0fb5-41ab-a14c-5391e1fd70a5

Title: Citrix Netscaler Attack CVE-2019-19781
- description: Detects CVE-2019-19781 exploitation attempt against Citrix Netscaler, Application Delivery Controller and Citri
- category: data/rules/web
- level: critical
- id: ac5a6409-8c89-44c2-8d64-668c29a2d756

Title: Solarwinds SUPERNOVA Webshell Access
- description: Detects access to SUPERNOVA webshell as described in Guidepoint report
- category: data/rules/web
- level: critical
- id: a2cee20b-eacc-459f-861d-c02e5d12f1db

Title: Successful Exchange ProxyShell Attack
- description: Detects URP patterns and status codes that indicate a successful ProxyShell exploitation attack against Exchang
- category: data/rules/web
- level: critical
- id: 992be1eb-e5da-437e-9a54-6d13b57bb4d8

Title: Fortinet CVE-2018-13379 Exploitation
- description: Detects CVE-2018-13379 exploitation attempt against Fortinet SSL VPNs
- category: data/rules/web
- level: critical
- id: a2e97350-4285-43f2-a63f-d0daff291738