SNYPR 6.2

OPERATING SYSTEM

Securonix Proprietary Statement

This material constitutes proprietary and trade secret information of Securonix, and shall not be disclosed to any third party, nor used by the recipient except under the terms and conditions prescribed by Securonix.

The trademarks, service marks, and logos of Securonix and others used herein are the property of Securonix or their respective owners.

Securonix Copyright Statement

Contact Information

Securonix, Inc.
14665 Midway Rd. Ste. 100, Addison, TX 75001
www.securonix.com
855.732.6649

Revision History

Date	Product Version	Description
5/17/2018	6.2	First Release
5/15/2018	6.2	Guide Update

Table of Contents

Operating System (OS)

This guide provides information about operating system (OS) functionalities, including:

- Required attributes (to support the use cases for this functionality),
- Threat focus areas, and
- Available policies.

What is Operating System?

An operating system software allows a user to run multiple applications on a computing device and manages a computer's hardware resources such as:

- Input devices (e.g. a keyboard and mouse),
- Output devices (e.g. display monitors, printers, and scanners),
- Network devices (e.g. modems, routers, and network connections), and
- Storage devices (e.g. internal and external drives)

The OS also provides services to facilitate the efficient execution and management of, and memory allocations for, any additional installed software application programs.

Sample Data Sources

- Cisco NX-OS
- IBM General Parallel File System
- ManageEngine ADAudit Plus
- Unix

Required Attributes

SNYPR parses and normalizes data into meaningful attributes for consistent representation of logging output from disparate devices and applications using Securonix Open Event Format (OEF) 1.0. OEF is an event interoperability standard/schema. This allows SNYPR to run uses cases across all datasources of the same functionality.

The following attributes are required to support the use cases included out-of-the-box with Operating System datasources for the Microsoft Windows device categorization:

Device Attribute	SNYPR Attribute
AccountName	accountname
Changed Attributes.User Workstations, Trust Information.Forest Root, Attributes.Profile Path	additionaldetails7
Changed Attributes.Account Expires	additionaldetails9
EventID	baseeventid
Subject.Logon Type	customnumber1
DateTime	DATETIME
Remote Endpoint.Network Address, Remote Endpoint.Private Address, Network Information.Remote IP Address, Network Information.Network Address, Network Information.Client Address, Attributes.User Workstations	destinationaddress
Network Information.Workstation Name, Target Server.Target Server Name, Additional Information.Caller Workstation, Additional Information.Caller Computer Name	destinationhostname

New Computer Account.Account Domain, Subject.Client Domain, Directory Service.Name, Account Whose Credentials Were Used.Account Domain, New Logon.Account Domain, Target Account.Account Domain, Account Information.Supplied Realm Name, New Account.Account Domain, Account For Which Logon Failed.Account Domain	destinationntdomain
ProcessInformationNewProcessName, DetailedAuthenticationInformationLogonProcessName, ServiceInformationServiceName, RPCAttributesAuthenticationServiceName	destinationprocessname
New Logon.Security ID, Account That Was Locked Out.Security ID, Target Account.Security ID, Member.Security ID, Account Information.User ID, New Account.Security ID, Account For Which Logon Failed.Security ID	destinationuserid
New Computer Account.Account Name, Changed Attributes.SAM Account Name, Subject.Client Name, Attribute.LDAP Display Name, Account Whose Credentials Were Used.Account Name, New Logon.Account Name, Account That Was Locked Out.Account Name, Target Account.Account Name, Member.Account Name, Account Information.Account Name, New Account.Account Name, Account For Which Logon Failed.Account Name	destinationusername
Client Machine.Account Name	destinationusername
Device Address	deviceaddress
Deleted Group.Group Name, Policy Change Details.Category, Operation.Accesses, Trusted Domain.Domain Name, Authentication Policy Information.Policy Name, Target Account.Additional Information, Group.Group Name, Additional Information.Ticket Options, New Group.Group Name, LogonTypeDescription	devicecustomstring1
Deleted Group.Group Domain, Policy Change Details.Subcategory, Object.Object Type, Group.Group Domain, Audit Policy Change.Category, Additional Information.Result Code, Object.Name, Object.Object Name, New Group.Group Domain	devicecustomstring2
Deleted Group.Security ID, New Group.Security ID, Audit Policy Change.Changes, Policy Change Details.Changes, Trusted Domain.Domain ID, Group.Security ID, Audit Policy Change.Subcategory, Object.Type, Failure Information.Failure Reason	devicecustomstring3
Detailed Authentication Information.Authentication Package, Change Information.Old Value	devicecustomstring4
Detailed Authentication Information.Package Name (NTLM only), Change Information.New Value	devicecustomstring5
FailureDescription	devicecustomstring6
EventLogType	eventoutcome

Object.File Name, Link Information.File Name	filename
Link Information.Link Name, ProcessInformationNewProcessPath, DetailedAuthenticationInformationLogonProcessPath, ServiceInformationServicePath, RPCAttributesAuthenticationServicePath	filepath
Process Information.Token Elevation Type	filepermission
New Logon.Logon ID	FlowSiemId
ipaddress	ipaddress
AdditionalDetails	message
ProcessInformationProcessPath, ProcessInformationCallerProcessPath, ProcessProcessPath, ProcessInformationCreatorProcessPath	oldfilepath
Application Information.Application Name, Attributes.UserAgent	requestclientapplication
Additional Information.Authentication Method	requestmethod
Network Information.Source Network Address, Local Endpoint.Network Address, Workstation Name.Source Network Address	sourceaddress
User.Account Domain, Subject.Account Domain	sourcentdomain
Network Information.Source Port, Workstation Name.Source Port	sourceport
Process.Process ID, Process Information.Process ID, Process Information.New Process ID, Process Information.Caller Process ID	sourceprocessid
ProcessInformationProcessName, ProcessInformationCallerProcessName, ProcessProcessName, ProcessInformationCreatorProcessName	sourceprocessname
User.Account Name, Subject.Account Name	sourceusername
Attributes.User Account Control, Additional Information.Privileges	sourceuserprivileges
SourceName_A	transactionstring1

What Policies are Provided?

Policies is the term used by Securonix to indicate the checks that must be run on each device to detect these threat indicators. Checks may include various types of analytical techniques.

Threat Focus Areas

Operating System policies, or use cases, include the policies for the following categories of threat:

Insider Threat: Attacks in which an employee gains access to network resources to steal or alter sensitive company data or introduce malware into the system.

Threat Categories:

- Alert
- Data Exfiltration
- Identity Issue
- Account Misuse

Cyber Threat: Attacks that targets computer information systems, infrastructures, computer networks, and/or personal computer devices.

Threat Categories:

- Alert
- Data Exfiltration
- Malware
- Account Misuse

Policies by Threat Category

Threat Category	Policy Name	Description
Account Misuse	Abnormal Number of Account Creation	This may be indicative of a privilege misuse activity
	Abnormal Number of Account Creation–Disabled	This may be indicative of a privilege misuse activity
	Abnormal Number of Account Creation–SIEM-13	Detects spike in amount of accounts created and disabled that may be indicative of a privilege misuse activity
	Abnormal Number of Account Lockout Events	Abnormal number of account lockout events could be indicative of a possible bruteforce event.
	Abnormal Number of Account Lockouts–SIEM-13	Abnormal number of account lockout events could be indicative of a possible bruteforce event.
	Abnormal Number of Accounts Enumerated	This could indicate a possible LDAP scanning event caused by a malicious presence. Enumeration of accounts is typically leveraged by malware for account takeover
	Abnormal Number of Administrative Share Object Accessed–SIEM-13	A spike in account accessing administrative share objects may be indicative of recon activity to exploit an endpoint
	Abnormal Number of Domain Password Reset Attempts	This could indicate a possible account takeover attempt. Unauthorized password changes on multiple accounts could also indicate denial of service.
	Abnormal Number of Hosts Accessed–SIEM-13	High number of hosts accessed during successful authentication events or run-as events may be indicative of malicious insider/cyber laterally propagating across multiple hosts using elevated credentials.
	Abnormal Number of Kerberos Pre-Authentication Failures–SIEM-13	Abnormal number of Kerberos pre authentication failures could be indicative of a possible bruteforce event.
	Abnormal Number of Logon Failures from an Account–SIEM-13	Abnormal number of logon failures could be indicative of a possible account takeover attempt. Logon failure reason could further indicate the severity of this attack

	Abnormal Number of Logon Failures–SIEM-13	Abnormal number of logon failures could be indicative of a possible account takeover attempt. Logon failure reason could further indicate the severity of this attack
	Abnormal Number of Password Resets	This may be indicative of a possible account takeover attempt. Unauthorized password changes on multiple accounts could also indicate denial of service.
	Abnormal Number of Password Resets–SIEM-13	This may be indicative of a possible account takeover attempt. Unauthorized password changes on multiple accounts could also indicate denial of service.
	Abnormal Number of Privileges Enumerated	This could indicate a possible LDAP scanning event caused by a malicious presence. Enumeration of privileges is typically leveraged by malwares to achieve privilege escalation
	Abnormal Number of Remote Logon Attempts	This policy detects a spike in successful remote interactive logons which could indicate lateral movement
	Abnormal Number of Remote Logon Attempts–SIEM-13	This policy detects a spike in successful remote interactive logons which could indicate lateral movement
	Abnormal Number of Run-as Activity–SIEM-13	Detects remote interactive logins, which is a technique malicious attackers use to laterally move across a network.
	Abnormal Number of Service Tickets Requested–SIEM-13	Abnormal number of server access requests
	Abnormal Number of Successful Authentication Attempts	A spike in the number of successful logins for a user account can indicate account misuse through password/account sharing, which as a best practice is a corporate policy violation or lateral movement if there are many remote interactive logins
	Abnormal Object or Network Share Access Attempts–SIEM-13	A spike in account accessing new network objects may be indicative of a possible snooping or a recon activity
	Account Added and Removed to Security Group	These temporary privilege escalation events may be indicative of a possible backdoor access attempt to use elevated privileges

	Account Created and Deleted	Temporarily creating and deleting an account may be indicative of a possible backdoor access attempt to use elevated privileges
	Account Enabled and Disabled	Temporarily enabling and disabling an account may be indicative of a possible backdoor access attempt to use elevated privileges
	Audit Log Tampering	Audit log tampering may be an attempt by a malicious entity to clear tracks involving unauthorized activity.
	Detection of Domain Trust Additions–Peer Anomaly	Unauthorized trust additions on a domain may be indicative of a possible privilege abuse and could lead to unauthorized access to services and resources
	Domain Account Creation by Users	Detects a normal user creating a domain account that could indicate an attacker creating and account to use directly.
	Firewall Configurations Modified on Windows	Modifying firewall configurations on an endpoint can cause a host to be vulnerable to exploits. It could also indicate a malicious entity attempting to disable firewall.
	Firewall Disabled on Windows	Disabling firewall on an endpoint can cause a host to be vulnerable to exploits. It could also indicate a malicious entity attempting to disable firewall.
	High Number of Failed Logins from an Undocumented Account	Detects high number of failed logins from undocumented account that could indicate an attacker attempting to gain access to the environment via a bruteforce.
	Local Accounts Created on Windows	Locally created accounts can't be monitored by the Domain Controller and can be leveraged to avoid defense mechanisms or create backdoors for future malicious use.
	Local Accounts Created on Windows–Target Domain Analysis	Locally created accounts can't be monitored by the Domain Controller and can be leveraged to avoid defense mechanisms or create backdoors for future malicious use.
	Member Added to Built-In Admin Groups by Uncorrelated Accounts	Adding members to built-in admin group could indicate a possible privilege escalation.
	New Admin Account Detected	Undocumented admin authentication could indicate a malicious activity.

	Pass the Hash Detection–Key Length Analysis	This is an indicator of lateral movement being observed via the pass the hash technique.
	Pass the Hash Detection–Randomly Generated Hosts	Detects pass the hash from randomly generated hosts.
	Password Reset Anomaly	This may be indicative of a possible account takeover attempt as these are not self-password reset events
	Possible Password Spraying from a Resource	A bruteforce attempt from a source host, whereby the same password wis tried against a list of user accounts.
	Possible Password Spraying from an IP Address	Possible brute force attempt to logon to an account
	Possible Privilege Escalation–Self Escalation	This may be indicative of a privilege abuse activity by users to escalate privileges on their local accounts
	Possible Remote Interactive Logon Enumeration	Enumeration behavior observed on interactive logon
	Rare Account Enumeration Event	This policy detects the occurrence of an account enumeration event for the first time
	Rare Admin Group Member Additions by User Compared to Peer	Rare admin group member additions compared to peers could be indicative of privilege misuse activity
	Rare Admin Share Access by an Account	This may be indicative of an account accessing new network objects could indicate a possible snooping or a recon activity
	Rare Audit Log Clearing by an Account	This may be indicative of an audit log tampering activity
	Rare Authentication Domain Detected	Detects authentication from a rare domain that can indicate account misuse or an attacker sneaking in through a trusted domain that has been added.
	Rare Built-in Member Group Additions	Detects rare built-in member group additions that could indicate an attacker elevating an account with addition rights, if a local machine account they are attempting to circumvent controls by hiding activities from the domain due to only being logged in the workstation logs.

	Rare Host Accessed Attempt by Account	A rare login attempt activity by account indicate a possible account takeover or a lateral propagation attempt
	Rare Host Accessed by an Account	A spike in account accessing new hosts could indicate a possible account takeover or a lateral propagation attempt
	Rare Host Accessed by an Account–Logon Failure	A spike in account accessing new hosts could indicate a possible account takeover or a lateral propagation attempt
	Rare Host Accessed from an Account	Detects that the account has accessed a system they would not normally, which can be an indicator of insider taking advantage of those privileges or more malicious activity.
	Rare Interactive Logon by Service Account	Rare interactive logon for a service account indicates a change in the typical authentication pattern for a service account. This could indicate an account being misused or using unauthorized elevated privileges.
	Rare Local Account Created	This policy detects the creation of a local account for the first time
	Rare Object Access Attempts by an Account	This may be indicative of an account accessing new network objects could indicate a possible snooping or a recon activity
	Rare Password Reset for Domain Admin	Rare password reset for domain admin may be indicative of a possible account takeover attempt.
	Rare Privilege Enumeration Event	This policy detects the occurrence of enumerating privileges for an account for the first time
	Rare Privileged Events Performed by User Compared to Peer	This may be indicative of a privilege misuse activity
	Rare Regedit Usage Compared to Peer	Rare registry modification attempts may be indicative of a possible circumvention of control activity or a malicious presence on the endpoint
	Rare Registry Modification by an Account	Rare registry modification attempts may be indicative of a possible circumvention of control activity or a malicious presence on the endpoint
	Rare Target Account Authentication Using Explicit Credentials	Rare target account during explicit credentials, could indicate a malicious entity attempting to

		impersonate as another account using elevated privileges.
	Scheduled Task Creation	Detects when tasks are scheduled. Scheduled tasks should be monitored as they can indicate an attacker creating persistence or an insider threat scheduling a task to occur.
	Service Account Performing Interactive Logon	Service accounts are typically only used for batched or application tasks. Interactive logon from these accounts could indicate a potential misuse or bypass of controls
	Suspicious Account Activity–Kerberoasting–Peak TGS Request for User Analytic	This event is an indication of an attacker collecting Kerberos Service Tickets for decryption to impersonate the embedded service accounts.
	Suspicious Account Activity–Kerberoasting–Rare TGS Encryption Type for User Analytic	Detects a rare service ticket granted encryption usage.
	Suspicious Account Activity–Peak Credential Validation Failure Increase for Host Analytic	Detects spike in enumeration of accounts with failed login from a single host as compared to its daily profile
	Suspicious Account Activity–Peak Explicit Credentials Distinct Account Name for Host Analytic	Detects a spike in enumeration of accounts using explicit credentials form a single user as compared to their daily profile
	Suspicious Account Activity–Potential Pass-the-Hash–Host Length Analytic	Detects rare potential pass the hash via host length events
	Suspicious Account Activity–Potential Pass-the-Hash–Key Length Analytic	Detects potential pass the hash via key-length
	Suspicious AD Enumeration Observed	Detects security enabled local group enumeration
	Suspicious AD Policy Change	Detects a change in AD policy by an account
	Suspicious Executables on a Machine	Detects a suspicious executable process started on a host
	Suspicious Host Access Behavior from an Account	Detects when a user attempts access multiple hosts as compared to the user's daily profile

	Suspicious Process Activity–Endpoint–Potential Mimikatz Object Handling Activity Analytic	Generates a violation when mimkatz object handling is observed.
	Suspicious Process Activity–Potential Mimikatz or Hash Passing Token Creation–Powershell Privileged Service Call Analytic	Generates a violation when powershell passes the hash
	Suspicious Registry Modification Observed	Generates a violation when registry key value modifications are observed.
	Suspicious Service Creation	This policy determines a user running a process/service on their machine not seen before
	Unusual High Number of Network Shares Accessed–SIEM	Detects unusual high number of network shares accessed, which could indicate a possible attacker looking for data to carry out objectives against such as exfiltration.
	Use of Explicit Credentials–Account Sharing or Password Misuse	Explicit usage of another user's credentials could indicate a account takeover or a password sharing activity
	Abnormal Number of Failed SSH Authentication Attempts–Activity Account	This is a behavior-based policy that detects spike in the number of failed SSH logins for a particular account
	Abnormal Number of Login Failures–SU	This is a behavior-based policy that detects spike in the number of failed SU authentication logins for a particular account
	Activity on a Rare Hostname Never Connected Before	This policy detects account logging on successfully to a host never connected before.
	Activity Performed by Terminated Account	This policy detects users performing activity post their termination
	Detect Audit Log Tampering	This policy detects unauthorized modifications to Unix log files
	Detect Password Retrieval from System Files	This policy detects accounts attempting to retrieve passwords from /etc/passwd and /etc/shadow files
	Detect Presence and Attempted Use of the Telnet Utility	This policy detects attempted use of the telnet utility
	Detect Use of XTERM, XWindows by User	This policy detects accounts using XTerm/XWindows

	Successful Authentication to Multiple Destination Hosts in a Short Period of Time–Activity Account	This policy detects accounts performing successful SSH login from single source host to at least 5 destination hosts within a duration of one hour
	User Emailing Files to External Email Addresses	This policy detects users using mail service on Unix hosts to email externally
Malware	Abnormal Number of Account Enumeration Attempts on an Endpoint	High number of accounts used during failed authentication events or lockout events may be indicative of malicious insider/cyber attempting to guess passwords for accounts.
	Abnormal Number of Kerberos Impersonation Attempts Detected–SIEM-13	This event is an indication of an attacker collecting Kerberos Service Tickets to impersonate the embedded service accounts.
	Abnormal number of Kerberos Pre-Authentication Failures	Abnormal number of Kerberos pre-authentication failures could be indicative of a possible bruteforce event.
	Abnormal Number of Logon Failures	Abnormal number of logon failures could be indicative of a possible account takeover attempt. Logon failure reason could further indicate the severity of this attack
	Abnormal Number of Network Share Object Access	A spike in account accessing new network objects may be indicative of a possible snooping or a recon activity
	Abnormal Number of Process Execution Using Explicit Credentials	A spike in run-as activity may be indicative of an account that might be laterally propagating using other accounts and running processes using those accounts
	Abnormal Number of Remote Logon Attempts	This policy detects a spike in successful remote interactive logons which could indicate lateral movement
	Detection of Possible Backdoor	Possible backdoor detected in the system. Backdoor is a sign of system compromise.
	High Number of Accounts from the Same IP Address for Successful Authentications or Run as Events	Detects high number of successful authentication events from the same ipaddress that could indicate successful lateral movement in an environment.
	High Number of Accounts Used on a Workstation for Successful Authentications or Run as Events	Detects high number of successful authentication or run-as events on a workstation that could indicate successful lateral movement in an environment.

	Password Hash Access	The password hash access event may be indicative of an attempt to take over the account whose password hash was accessed.
	Possible AD Enumeration	This may be indicative of a possible LDAP scanning event caused by a malicious presence. Enumeration of privileges is typically leveraged by malwares to achieve privilege escalation.
	Possible Impersonation Detected	Detects events that may indicate an attacker is collecting Kerberos Service Tickets for decryption to impersonate the embedded service accounts.
	Possible Privilege Enumeration	This may be indicative of a possible LDAP scanning event caused by a malicious presence. Enumeration of privileges is typically leveraged by malwares to achieve privilege escalation.
	Rare Basic Service Operation	Detects basic service operations that haven't been seen before.
	Rare Logon Process Detected for Windows Authentication	Rare logon process for an account indicates a change in the typical authentication pattern for an account. This could indicate an account being misused or using unauthorized elevated privileges.
	Rare Logon Type Detected for an Account	Rare logon type for an account indicates a change in the typical authentication pattern for an account. This could indicate an account being misused or using unauthorized elevated privileges
	Rare Privileged Level for Windows Authentication	Rare privilege level for a new logon indicates a change in the typical authentication pattern for an account. This could indicate an account being misused or using unauthorized elevated privileges.
	Rare Process Creation on an Endpoint	This anomaly may be indicative of a possible malicious process being executed, additional indicators like path of execution would determine the severity.
	Rare Process Detected for Authentication Using Explicit Credentials	Rare process for authentication using explicit credentials could indicate an authentication with elevated privileges. This type of activity coupled with other authentication anomalies could indicate lateral propagation
	Rare Process Spawned by a Parent Process	This anomaly may be indicative of a possible malicious process being executed, additional

		indicators like path of execution would determine the severity.
	Rare Token Elevation for Process	Rare token elevation for a process could indicate a process created with elevated privileges. This process can be used by a malicious actor to exploit a vulnerability
	Replay Attack Detection	A replay attack occurs when an intruder steals a packet from the network and forwards that packet to a service or application as if the intruder was the user who originally sent the packet. When the packet is an authentication packet, the intruder can use the replay attack to authenticate on another person's behalf and consequently access that person's resources or data.
	Spike in Administrative Shares Accessed	A spike in account accessing administrative share objects may be indicative of recon activity to exploit an endpoint
	Unusual Service Authentication Detected for User	Rare logon type for an account indicates a change in the typical authentication pattern for an account. This could indicate an account being misused or using unauthorized elevated privileges
	Use of Credential Dumpers	Credential dumpers usage is detected. It's used to extract credential hashes for offline cracking, extracting plaintext passwords, and extracting Kerberos tickets, among others.
Alert	A Member was Added and Removed from a Security-Enabled Group within a Short Time–13	Temporarily creating and deleting an account may be indicative of a possible backdoor access attempt to use elevated privileges
	Abnormal Number of Administrative Share Object Accessed	A spike in account accessing administrative share objects may be indicative of recon activity to exploit an endpoint
	Abnormal Number of Failed Logons from an IP Address–SIEM–13	High number of failed logons observed from an ipaddress
	Abnormal Number of Failed Logons on a Resource–SIEM–13	High number of failed logons observed from a resource
	Abnormal Number of Hosts Accessed	High number of hosts accessed during successful authentication events or run-as events may be indicative of malicious insider/cyber laterally

		propagating across multiple hosts using elevated credentials.
	Abnormal Number of Remote Interactive Logon from an Account–SIEM–13	Anomalous number of remote interactive logon from an account
	Abnormal Object or Network Share Access Attempts by Resource–SIEM–13	Detects multiple network object access that could indicate an attacker snooping and collecting data for exfiltration.
	Audit Policy Changes	This may be indicative of an audit log tampering activity
	Certificate Service Status	A certificate service stopped could indicate malicious activity. This should be coupled with other endpoint, authentication or network anomalies.
	Logging User Account Disabled	Monitors disabling of service accounts used for logging purposes
	Multiple Failed Logons	Repeated failed authentication events may be indicative of a malicious entity attempting to communicate to a Command and Control server or to receiving the malicious payload.
	Possible Bruteforce Attempt–13	Failed logon attempts followed by successful logons
	Remote Interactive Logon to Domain Controller by Non-Admin Account	Detects remote logins to domain controllers by non-admins accounts that could indicate an attacker performing recon to determine what entity to move to next in the environment.
	Restricted Group Change	These restricted group change events may be indicative of a possible backdoor access attempt.
	Suspicious Logon Attempts	Sysadmin authentication could indicate a malicious activity.
	Suspicious Process Activity–Log Clearing Analytics	Generates a violation when event logs are cleared
	Use of Any Default Credentials	Detects any use of default credentials that can indicate account misuse or an attacker in the environment attempting to carry out objects on target.
	Windows Account Lockouts	Detects multiple account lockouts that can indicate a denial of service by an attacker.

Identity Issue	Windows Activity by Terminated Accounts	Activity by terminated users may be indicative of a possible account misuse or a gap in the deprovisioning process
Data Exfiltration	Possible Local Account Created	Accounts created on a rare domain could be possible local accounts and can't be monitored by the Domain Controller and which can be leveraged to avoid defense mechanisms or create backdoors for future malicious use.
Alert, Malware	Abnormal Number of Host Access Attempts	High number of hosts accessed during failed authentication events or lockout events may be indicative of malicious insider/cyber attempting to laterally propagate across multiple hosts.
Alert, Account Misuse	Rare Host Accessed by an Account– Logon Success	A spike in account accessing new hosts could indicate a possible account takeover or a lateral propagation attempt
Account Misuse, Malware	Rare Service Created on Endpoint	This anomaly may be indicative of a possible malicious service being executed, additional indicators like path of execution would determine the severity.

Policy Details

Abnormal Number of Account Creation

Criticality: Low
Applies to: Functionality
Policy Category: Account Misuse

Device Category

Windows

Description

This may be indicative of a privilege misuse activity

Technique Used

Behavior anomaly on account creation activity

Analytical Type

Tier 2 Behavior Summary

Prerequisites

- windows logs
- Behavior profiles
- Naming Convention for Domain admin Accounts

Violation Entity

Resource Group Account

Threat Focus Area
Insider/Cyber

Threat Indicator
Possible privilege misuse

Kill Chain Stage
Recon

Remediation Steps
Possible steps for further analysis/triage to consider:

1. Determine if the activity is approved by checking service management system for an incident/work order (ticket) associated with the activity. Domain Admins may have several tickets to create new accounts.
2. Determine if the created account activities are anomalies or expected.
3. Determine if the source account has other anomalies.
4. Determine if the source account or its peers have performed similar activities.

Possible Remediation steps after further analysis and triage:

1. Submit a ticket to revert any changes made.
2. Submit a ticket to disable the account(s).
3. Submit a ticket to remove the account(s) (as needed)
4. Submit a ticket to revoke privileges.

Detection Algorithm
Spike in Number of Occurrences

Criteria to Filter Event
baseeventid equal to 624 [or]
baseeventid equal to 4720
And
Account Name does not contain $ [and]
Account Name not equal to ANONYMOUS LOGON [and]
Account Name does not contain LOCAL [and]
Account Name not equal to –

Verbose Info

Account: ${accountname!"ACCOUNTNAME"} on Host: ${resourcename!"UNKNOWN"} created Users: ${destinationusername$LIST!"UNKNOWN"} for Domain: ${destinationntdomain!"UNKNOWN"} Message: ${message!"UNKNOWN"} EventID: ${baseeventid!"UNKNOWN"}

Response Bot Fields/Attributes/Policies

Abnormal number of account creation-SIEM-13
Account added and removed to security group
Account Created and Deleted
Local accounts created on windows - Target domain analysis
Rare local account created
Abnormal number of account creation-disabled
Possible local account created
Domain account creation by users
Local accounts created on windows
Account Created and Deleted-13

DISTCOUNT (destinationusername) - Count of unique users created
DISTCOUNT (destinationntdomain) - Count of unique domains for which users were created

---

Abnormal Number of Account Creation–Disabled

Criticality: Low
Applies to: Functionality
Policy Category: Account Misuse

Device Category

Windows

Description

This may be indicative of a privilege misuse activity

Technique Used

Behavior anomaly on account creation activity

Analytical Type

Tier 2 Behavior Summary

Prerequisites

- windows logs
- Behavior profiles
- Naming Convention for Domain admin Accounts

Violation Entity

Activity Account

Threat Focus Area

Insider/Cyber

Threat Indicator

Possible privilege misuse

Kill Chain Stage
Recon

Remediation Steps
AD BlockUser; AD UnBlockUser

Detection Algorithm
Spike in Volume/amount

Criteria to Filter Event
baseeventid equal to 624 [or]
baseeventid equal to 4720

Risk Boosters
Active List:
Suspicious_host_accessed increase factor 4.0
Possible_Brutefore increase factor 4.0
Suspicious_process_anomaly increase factor 4.0
Suspicious_AD_Authentication increase factor 4.0
Possible_privilege_misuse increase factor 4.0
Vulnerable_endpoints increase factor 4.0
Infected_endpoints increase factor 4.0

Verbose Info
Account ${accountname!"ACCOUNTNAME"} performed ${transactionstring1!"ACTIVITY"} from ipaddress ${ipaddress!"UNKNOWN"}

Response Bot Fields/Attributes/Policies
Abnormal number of account creation-SIEM-13
Account Created and Deleted
Account Enabled and Disabled
Local accounts created on windows - Target domain analysis
Rare local account created
Logging User Account Disabled
Possible local account created
Local accounts created on windows

Abnormal Number of Account Creation–SIEM-13
Criticality: Low
Applies to: Functionality
Policy Category: Account Misuse

Device Category
Windows

Description
Detects spike in amount of accounts created and disabled that may be indicative of a privilege misuse activity

Analytical Type
Directive Based

Prerequisites
- windows logs

Violation Entity
Resource Group Account

Threat Focus Area
Insider/Cyber

Threat Indicator
Possible privilege misuse

Kill Chain Stage
Recon

Remediation Steps
Possible steps for further analysis/triage to consider:

1. Determine if the activity is approved by checking service management system for an incident/work order (ticket) associated with the activity. Domain Admins may have several tickets to create new accounts.
2. Determine if the created account activities are anomalies or expected.
3. Determine if the source account has other anomalies.
4. Determine if the source account or its peers have performed similar activities.

Possible Remediation steps after further analysis and triage:

1. Submit a ticket to revert any changes made.
2. Submit a ticket to disable the account(s).
3. Submit a ticket to remove the account(s) (as needed)
4. Submit a ticket to revoke privileges

Detection Algorithm
Aggregated event analytics

Criteria to Filter Event
Account Name is not null [and]
baseeventid equal to 4720 [and]
Account Name dose not contain svc [and]
account name not equal to -
account name does not contain $ [and]
account name not equal to NA [and}
account name does not contain system [and]
account name does not contina ANONYMOUS LOGON [and]
account name does not contain Window Manager [and]
account name does not contain DWM

Directives
Name Abnormal number of account creation
Filter for Events matching criteria? baseeventid CONDITION_EQUALS 4720
Having similar accountname
Number of Occurrences 10
Within Duration 00:59:59
Should events happen consecutively? false
Distinct? Destinationusername

Verbose Info
Account: ${accountname!"ACCOUNTNAME"} on Host: ${resourcename!"UNKNOWN"} created Users: ${destinationusername$LIST!"UNKNOWN"} for Domain: ${destinationntdomain!"UNKNOWN"} Message: ${message!"UNKNOWN"} EventID: ${baseeventid!"UNKNOWN"}

Response Bot Fields/Attributes/Policies
Account Created and Deleted-13
Account Created and Deleted
Local accounts created on windows - Target domain analysis
Abnormal number of account creation
Abnormal number of account creation-disabled
Possible local account created
Domain account creation by users
Local accounts created on windows
Rare local account created

DISTCOUNT (destinationusername) - Count of unique users created
DISTCOUNT (destinationntdomain) - Count of unique domains for which users were created

---

Abnormal Number of Account Lockout Events
Criticality: Low
Applies to: Functionality
Policy Category: Account Misuse

Device Category
Windows

Description
Abnormal number of account lockout events could be indicative of a possible bruteforce event.

Technique Used
Behavior anomaly on the account lockout activity for an account

Analytical Type
Tier 2 Behavior Summary

Prerequisites
- windows logs
- Behavior profiles
- Host Peer correlation: Department
- Client Naming conventions

Violation Entity
Resource Group Account

Threat Focus Area
Insider/Cyber

Threat Indicator
Suspicious AD Authentication

Kill Chain Stage

Recon

Remediation Steps

Possible further analysis/triage steps to consider:

1. Determine if the target account has any other anomalies
2. Determine If there are any successful logins against the target account.
3. Determine if the Target account's peers have any anomalies associated.
4. Determine if there is a commonality between the resources, such as all belonging to one depart or specific set of users.
5. Determine if any of the sources has additional anomalies.

Possible Remediation steps after further analysis/triage:

1. If successful login observed, open ticket to disable and reset password for target account as it could be compromised.
2. If any host found to be malicious, Open ticket to Isolate / remediate system according to internal Incident Response playbook.

Detection Algorithm

Spike in Number of Occourences
Transactionstring1
Account lockout events-9
Transaction occurence abnormally higher than User's Daily behavior
Sigma 0.5

Criteria to Filter Event

baseeventid equal to 4740 [or]
baseeventid equal to 644
AND
Account Name does not contain LOCAL [and]
Account name does not contain $ [and]
account Name does not contain ANONYMOUS [and]
Account name not equal to –

Verbose Info

Account: ${accountname!"ACCOUNTNAME"} on Host: ${resourcename!"UNKNOWN"} triggered multiple lockouts for Destination User: ${destinationusername$LIST!"UNKNOWN"} Message: ${message!"UNKNOWN"} EventID: ${baseeventid!"UNKNOWN"}

Response Bot Fields/Attributes/Policies

Abnormal number of account lockouts-SIEM-13
High number of accounts from the same ipaddress for authentication failures or lockout events
Windows Account lockouts
Abnormal number of remote interactive logon from an account-SIEM-13
Abnormal number of failed logons from an ipaddress-SIEM-13
Abnormal number of kerberos pre authentication failures-SIEM-13
Abnormal number of logon failures-SIEM-13
Abnormal number of logon failures from an account-SIEM-13
Abnormal number of failed logons on a resource- SIEM-13
Multiple failed logons
Possible remote interactive logon enumeration
Possible password spraying from an ipaddress
Possible password spraying from a resource
Abnormal number of password resets
Abnormal number of kerberos pre authentication failures
Abnormal number of account enumeration attempts on an endpoint
Abnormal number of logon failures
Abnormal number of remote logon attempt
Rare host accessed by an account - Logon Failure
High Number of Failed Logins from an Undocumented Account
Possible Brute Force Attack VPN
Abnormal number of account lockouts-SIEM-17
Abnormal number of failed logons from an ipaddress-SIEM-17
Abnormal number of kerberos pre authentication failures-SIEM-17
Abnormal number of failed logons on a resource- SIEM-17

DISTCOUNT (destinationusername)

Abnormal Number of Account Lockouts–SIEM-13

Criticality: Low
Applies to: Functionality
Policy Category: Account Misuse

Device Category

Windows

Description

Abnormal number of account lockout events could be indicative of a possible bruteforce event.

Technique Used

Behavior anomaly on the account lockout activity for an account

Analytical Type

Directive Based

Prerequisites

- windows logs
- Behavior profiles
- Host Peer correlation: Department
- Client Naming conventions

Violation Entity

Resource Group Account

Threat Focus Area
Insider/Cyber

Threat Indicator
Suspicious AD Authentication

Kill Chain Stage
Recon

Remediation Steps
Possible further analysis/triage steps to consider:

1. Determine if the target account has any other anomalies
2. Determine If there are any successful logins against the target account.
3. Determine if the Target account's peers have any anomalies associated.
4. Determine if there is a commonality between the resources, such as all belonging to one depart or specific set of users.
5. Determine if any of the sources has additional anomalies.

Possible Remediation steps after further analysis/triage:

1. If successful login observed, open ticket to disable and reset password for target account as it could be compromised.
2. If any host found to be malicious, Open ticket to Isolate / remediate system according to internal Incident Response playbook.

Detection Algorithm
Aggregated event analytics

Criteria to Filter Event
Account name is not null [and]
account name does not contain $ [and]
baseeventid equal to 4740 [and}
account name does not contain ANONYMOUS [and]
account name does not contain LOCAL [and]
account name does not equal –

Directives
Name Abnormal Number of Account LockOuts
Filter for Events matching criteria? NA
Having similar accountname
Number of Occurrences 3
Within Duration 00:59:59
Should events happen consecutively? false
Distinct? NA

Verbose Info
Account: ${accountname!"ACCOUNTNAME"} on Host: ${resourcename!"UNKNOWN"} triggered multiple lockouts for Destination User: ${destinationusername$LIST!"UNKNOWN"} Message: ${message!"UNKNOWN"} EventID: ${baseeventid!"UNKNOWN"}

Response Bot Fields/Attributes/Policies

Abnormal number of failed logons from an ipaddress-SIEM-13
Abnormal number of kerberos pre authentication failures-SIEM-13
Abnormal number of logon failures-SIEM-13
Abnormal number of logon failures from an account-SIEM-13
Abnormal number of failed logons on a resource- SIEM-13
Multiple failed logons
Abnormal number of account lockout events
Abnormal number of kerberos pre authentication failures
High number of accounts from the same ipaddress for authentication failures or lockout events
Abnormal number of logon failures
Rare host accessed by an account - Logon Failure
High Number of Failed Logins from an Undocumented Account
Windows Account lockouts
Suspicious Account Activity - Peak Credential Validation Failure Increase For Host Analytic
Abnormal number of account lockouts-SIEM-17
Abnormal number of kerberos pre authentication failures-SIEM-17
Abnormal number of failed logons on a resource- SIEM-17
Abnormal number of remote logon attempts-SIEM-13
Possible password spraying from an ipaddress
Possible password spraying from a resource
Abnormal number of remote logon attempt
Abnormal number of remote logon attempts
Abnormal number of failed logons from an ipaddress-SIEM-17

DISTCOUNT (destinationusername)

Abnormal Number of Accounts Enumerated

Criticality: Low
Applies to: Functionality
Policy Category: Account Misuse

Device Category

Windows

Description

This could indicate a possible LDAP scanning event caused by a malicious presence. Enumeration of accounts is typically leveraged by malware for account takeover

Analytical Type

Tier 2 Behavior Summary

Prerequisites

- windows logs
- User Behavior profiles
- User naming conventions to identify users that may carryout

Violation Entity

Resource Group Account

Threat Focus Area

Cyber

Threat Indicator
possible account enumeration

Kill Chain Stage
Exploit

Remediation Steps
Possible steps for further analysis/triage to consider:

1. Determine if the activity is approved by checking service management system for an incident / work order (ticket) associated with the activity.
2. Determine if the target resources have any other anomalies.
3. Determine if the source account or its peers have performed similar activities.
4. Determine if the source account should be performing the activity via a role to privilege comparison.
5. Determine if the endpoint has other anomalies associated with its processes, sessions, or network connections.

Possible Remediation steps after further analysis and triage:

1. Submit a ticket to revert any changes that occurred.
2. Submit a ticket to disable the account.
3. Submit a ticket to remove the account (as needed)
4. Submit a ticket to revoke privileges
5. Submit a ticket to perform a full Antivirus scan
6. Submit a ticket for host isolation and further remediation as per internal IR playbooks dictate.

Detection Algorithm
Spike in Number of Occourences
transactionstring1
AccountEnumeration_Frequency
Transaction occurence abnormally higher than User's Daily behavior
Sigma 0.5

Criteria to Filter Event
baseeventid equal to 4798
AND
Account Name does not contain LOCAL [and]
Account name does not contain $ [and]
account Name does not contain ANONYMOUS [and]
Account name not equal to –

Verbose Info
Account: ${accountname!"ACCOUNTNAME"} from IP address: ${ipaddress!"UNKNOWN"} with Host name: ${resourcename!"UNKNOWN"} enumerated group membership for Usera: ${destinationusername$LIST!"UNKNOWN"} Message: ${message!"UNKNOWN"} EventID: ${baseeventid!"UNKNOWN"}Response Bot Fields/Attributes/Policies
Abnormal number of account creation-SIEM-13
Account added and removed to security group
Account Created and Deleted
Local accounts created on windows - Target domain analysis
Rare local account created
Abnormal number of account creation-disabled
Possible local account created
Domain account creation by users
Local accounts created on windows
Account Created and Deleted-13

DISTCOUNT (destinationusername) - Count of unique users created

DISTCOUNT (destinationntdomain) - Count of unique domains for which users were created

Response Bot Fields/Attributes/Policies

Possible AD Enumeration
Abnormal number of privileges enumerated
Rare account enumeration event
Rare privilege enumeration event
Abnormal number of account enumeration attempts on an endpoint
Possible Privilege Enumeration
Suspicious AD Enumeration Observed

DISTCOUNT (destinationusername)

Abnormal Number of Administrative Share Object Accessed–SIEM-13

Criticality: High
Applies to: Functionality
Policy Category: Account Misuse

Device Category

Windows

Description

A spike in account accessing administrative share objects may be indicative of recon activity to exploit an endpoint

Technique Used

Behavior anomaly on administrative share access activity

Analytical Type

Directive Based

Prerequisites

- Windows logs
- behavior profiles
- Server name conventions
- Service Account naming conventions

Violation Entity

Resource Group Account

Threat Focus Area

Cyber

Threat Indicator

Suspicious network share access

Kill Chain Stage

Recon

Remediation Steps

Possible steps for further analysis/triage to consider:

1. Determine if the activity is approved by checking service management system for an incident / work order (ticket) associated with the activity.
2. Determine if the account has other anomalies.
3. Determine if the account or its peers have performed similar activities.
4. Determine if the account should be performing the activity via a role to privilege comparison.
5. Determine if the endpoint has other anomalies associated with its processes, sessions, or network connections.
6. Determine if any of the processes and their hash values are malicious.

Possible Remediation steps after further analysis and triage:

1. Submit a ticket to revert any changes that occurred.
2. Submit a ticket to disable the account.
3. Submit a ticket to remove the account (as needed)
4. Submit a ticket to revoke privileges
5. Submit a ticket to perform a full Antivirus scan
6. Submit a ticket for host isolation and further remediation as per internal IR playbooks dictate.

Detection Algorithm

Aggregated Event Analytics

Criteria to Filter Event

account name does not contain $ [and]
account name is not null [and]
account name does not contain SVC [and]
baseeventid equal to 5140 [and]
resource CustomeField 5 contains admin [and]
source hostname does not contain ADS [and]
source hostname does not contain ADC [and]
Account name not equal to - [and]
account name not equal to NA [and]
account name does not contain SYSTEM [and]
account name does not contain DWM [and[]
account name does not contain ANONYMOUS LOGON [and]
account name does not contain Window Manager

Additional Event Analytics

Check agains Lookup Table:
Account name not equal to WhitelistedDomains
IPAddress not equal to WhitelistedDomains
resourcename not equal to WhitelistedDomains

Directives

Name Abnormal number of administrative share object accessed
Filter for Events matching criteria? baseeventid CONDITION_EQUALS 5140
Having similar accountname
Number of Occurrences 5
Within Duration 00:30:00
Should events happen consecutively? false
Distinct? NA

Risk Boosters

Match Criteria:
baseeventid = 5140 increase factor 2.0
resource CustomField 5 contains C$ or Contains ADMIN$ increase factor 3.0

Verbose Info

Account: ${accountname!"ACCOUNTNAME"} on Host: ${resourcename!"UNKNOWN"} accessed Shares: ${resourcecustomfield5$LIST!"UNKNOWN"} Message: ${message!"UNKNOWN"} EventID: ${baseeventid!"UNKNOWN"}

Response Bot Fields/Attributes/Policies

Abnormal object or network share access attempts by resource-SIEM-13
Abnormal number of hosts accessed-SIEM-13
Abnormal object or network share access attempts-SIEM-13
Rare host accessed by an account
Rare admin share access by an account
Abnormal number of network share object access
Abnormal number of host access attempts
Abnormal number of hosts accessed
Abnormal number of administrative share object accessed
Rare host accessed by an account - Logon Failure
Rare Host Accessed Attempt By Account
Rare Host Accessed from an Account
Suspicious host access behavior from an account
Rare object access attempts by an account
Abnormal number of hosts accessed-SIEM-17

COUNT (resourcecustomfield5)
DISTCOUNT (resourcecustomfield5)

Abnormal Number of Domain Password Reset Attempts

Criticality: Low
Applies to: Functionality
Policy Category: Account Misuse

Device Category

Windows

Description

This could indicate a possible account takeover attempt. Unauthorized password changes on multiple accounts could also indicate denial of service.

Analytical Type

Tier 2 Behavior Summary

Prerequisites

- windows logs
- Behavior profiles
- User naming conventions if default account names are changed

Violation Entity

Resource Group Account

Threat Focus Area

Insider/Cyber

Threat Indicator

Possible privilege MISUSE

Kill Chain Stage
Delivery

Remediation Steps
Possible steps for further analysis / triage to consider:

1. Determine if the activity is approved by checking service management system for an incident / work order (ticket) associated with the activity.
2. Determine if the target account has been logged into or has other anomalies.
3. Determine if the source account should be performing the activity via a role to privilege comparison.
4. Determine if the source account has any other anomalies
5. Determine if the endpoint has other anomalies associated with its processes, sessions, or network connections.

Possible Remediation steps after further analysis and triage:

1. Submit a ticket to revert any changes that occurred.
2. Submit a ticket to reset passwords / disable the account(s).
3. Submit a ticket to remove the account.
4. Submit a ticket to revoke privileges
5. Submit a ticket to isolate source host and investigate as per internal IR playbooks.

Detection Algorithm
Spike in Number of Occurrences
Transactionstring1
Transaction Occurrence Abnormally higher than User's Daily Behavior
sigma: 0.5

Criteria to Filter Event
baseid equal to 4794
AND
Account name not equal to - [and]
Account name does not contain $ [and]
account name does not contain LOCAL [and]
account name does not contain ANONYMOUS

Verbose Info
Account: ${accountname!"ACCOUNTNAME"} on Host: ${resourcename!"UNKNOWN"} reset password for User: ${destinationusername!"UNKNOWN"} Message: ${message!"UNKNOWN"} EventID: ${baseeventid!"UNKNOWN"}

Response Bot Fields/Attributes/Policies
Abnormal number of domain password reset attempts-SIEM-13
Abnormal number of password resets-SIEM-13
Abnormal number of password resets
Password Reset Anomaly
Rare password reset for domain admin
Abnormal number of domain password reset attempts-SIEM-17

Abnormal Number of Hosts Accessed–SIEM-13
Criticality: Low
Applies to: Functionality
Policy Category: Account Misuse

Device Category
Windows

Description
High number of hosts accessed during successful authentication events or run-as events may be indicative of malicious insider/cyber laterally propagating across multiple hosts using elevated credentials.

Analytical Type
Directive Based

Prerequisites
- windows logs
- Naming conventions for hosts

Violation Entity
Resource Group Account

Threat Focus Area
Insider/Cyber

Threat Indicator
Suspicious AD Authentication

Kill Chain Stage
Recon

Remediation Steps
Possible steps for further analysis / triage to consider:

1. Determine if the activity is approved by:
    - Checking service management system for an incident /work order (ticket) associated with the activity
    - Comparison to the user's peer group
    - Role to privilege comparison
2. Determine if the target accounts and resources have additional anomalies
3. Determine if the source account has other anomalies.
4. Determine if the endpoint has other anomalies associated with its processes, sessions, or network connections.

Possible Remediation steps after further analysis and triage:

1. Submit a ticket to revert any changes that occurred.
2. Submit a ticket to reset passwords / disable the account(s).
3. Submit a ticket to remove the account(s) (as needed)
4. Submit a ticket to revoke privileges
5. Submit a ticket to perform a full Antivirus scan
6. Submit a ticket for host isolation and further remediation as per internal IR playbooks dictate.

Detection Algorithm
Aggregated event analytics

Criteria to Filter Event
Account Name DOES NOT CONTAIN $ [and]
Account Name IS NOT NULL [and]
CustomNumber 1 CONTAINS 10 [and]
Account Name NOT EQUAL TO ANONYMOUS LOGON [and]
Account Name NOT EQUAL TO NA [and]
Account Name NOT EQUAL TO - [and]

Account Name DOES NOT CONTAIN SYSTEM [and]
Account Name DOES NOT CONTAIN DWM [and]
Account Name DOES NOT CONTAIN Window Manager [and]
AND
baseeventid EQUAL TO 4624 [or]
baseeventid EQUAL TO 528

Directives

Name Abnormal number of hosts accessed
Filter for Events matching criteria? NA
Having similar accountname
Number of Occurrences 5
Within Duration 00:30:00
Should events happen consecutively? false
Distinct? Sourcehostname

Risk Boosters

Match criteria:
baseeventid equal to 4624 [or]
baseeventid equal to 528
Increase factor 1.0

Verbose Info

Account: ${accountname!"ACCOUNTNAME"} IP address: ${ipaddress$LIST!"UNKNOWN"} Host: ${resourcename$LIST!"UNKNOWN"} Message: ${message!"UNKNOWN"} EventID: ${baseeventid!"UNKNOWN"}

Response Bot Fields/Attributes/Policies

Abnormal object or network share access attempts by resource-SIEM-13
Abnormal number of administrative share object accessed-SIEM-13
Abnormal object or network share access attempts-SIEM-13
Rare host accessed by an account
Rare admin share access by an account
Abnormal number of network share object access
Abnormal number of host access attempts
Abnormal number of hosts accessed
Abnormal number of administrative share object accessed
Rare host accessed by an account - Logon Success
Spike in administrative shares accessed
Rare host accessed by an account - Logon Failure
Rare Host Accessed Attempt By Account
Unusual high number of network shares accessed - SIEM
Rare Host Accessed from an Account
Suspicious host access behavior from an account
Rare object access attempts by an account
Abnormal number of administrative share object accessed-SIEM-17
Abnormal number of hosts accessed-SIEM-17

Abnormal Number of Kerberos Pre-Authentication Failures–SIEM-13

Criticality: Low
Applies to: Functionality
Policy Category: Account Misuse

Device Category
Windows

Description
Abnormal number of Kerberos pre authentication failures could be indicative of a possible bruteforce event.

Technique Used
Behavior anomaly on the Kerberos pre-authentication failures

Analytical Type
Directive Based

Prerequisites
- windows logs

Violation Entity
Activity Account

Threat Focus Area
Insider/Cyber

Threat Indicator
Suspicious AD Authentication

Kill Chain Stage
Recon

Remediation Steps
AD BlockUser; AD UnBlockUser; Tanium - Machine Information; Tanium - Running Applications; Tanium - Non-approved Established Connections

Detection Algorithm
Aggregated event analytics

Criteria to Filter Event
Account Name IS NOT NULL [and]
Account Name DOES NOT CONTAIN $ [and]
Account Name DOES NOT CONTAIN svc [and]
baseeventid EQUAL TO 4771 [and]
Account Name NOT EQUAL TO mfscanner [and]
Account Name NOT EQUAL TO mfprinter [and]
Account Name NOT EQUAL TO ANONYMOUS LOGON [and]
Account Name NOT EQUAL TO - [and]
Account Name DOES NOT CONTAIN SYSTEM [and]
Account Name NOT EQUAL TO NA [and]
Account Name DOES NOT CONTAIN DWM [and]
Account Name DOES NOT CONTAIN Window Manager

Directives
Name Abnormal number of kerberos pre authentication failures
Filter for Events matching criteria? NA
Having similar accountname

Number of Occurrences 35
Within Duration 00:59:59
Should events happen consecutively? false
Distinct? NA

Verbose Info

Account: ${accountname!"ACCOUNTNAME"} from IP address: ${ipaddress!"UNKNOWN"} Host: ${resourcename!"UNKNOWN"} had Message: ${message!"UNKNOWN"} EventID: ${baseeventid!"UNKNOWN"}

Response Bot Fields/Attributes/Policies

Abnormal number of Kerberos impersonation attempts detected-SIEM-13
Abnormal number of failed logons from an ipaddress-SIEM-13
Abnormal number of logon failures-SIEM-13
Abnormal number of remote logon attempts-SIEM-13
Abnormal number of logon failures from an account-SIEM-13
Abnormal number of failed logons on a resource- SIEM-13
Multiple failed logons
Abnormal number of logon failures
Suspicious Logon Attempts
Abnormal number of remote logon attempt
Rare host accessed by an account - Logon Failure
Abnormal number of remote logon attempts
Abnormal number of failed logons from an ipaddress-SIEM-17
Abnormal number of failed logons on a resource- SIEM-17
Suspicious Account Activity - Kerberoasting - Peak TGS Request For User Analytic
Suspicious Account Activity - Kerberoasting - Rare TGS Encryption Type For User Analytic
Suspicious Account Activity - Peak Credential Validation Failure Increase For Host Analytic

Abnormal Number of Logon Failures from an Account–SIEM-13

Criticality: None
Applies to: Functionality
Policy Category: Account Misuse

Device Category

Windows

Description

Abnormal number of logon failures could be indicative of a possible account takeover attempt. Logon failure reason could further indicate the severity of this attack

Technique Used

Behavior anomaly on the logon failure activity for an account

Analytical Type

Directive Based

Prerequisites

- windows logs
- Account naming convention if svc accounts are to be excluded

Violation Entity

Resource Group Account

Threat Focus Area

Cyber

Threat Indicator

Possible bruteforce

Kill Chain Stage

Recon

Remediation Steps

Possible further analysis/triage steps to consider:

1. Determine if the target account has any other anomalies
2. Determine If there are any successful logins against the target account.
3. Determine if the Target account's peers have any anomalies associated.
4. Determine if there is a commonality between the resources, such as all belonging to one depart or specific set of users.
5. Determine if any of the sources has additional anomalies.

Possible Remediation steps after further analysis/triage:

1. If successful login observed, open ticket to disable and reset password for target account as it could be compromised.
2. If any host found to be malicious, Open ticket to Isolate / remediate system according to internal Incident Response playbook.

Notes:

- If seen for a service account check to see if a password was recently changed as scripts could be hardcoded with the password and were not updated to reflect the change and thus it triggered an alert.
- Check if the primary resource causing failed logins is a mobile device assigned to the user. the device may caused failed logins / lockouts if the password is not properly synced when changed by a user.

Detection Algorithm

Aggregated Event Analytics

Criteria to Filter Event

Account Name IS NOT NULL [and]
Account Name DOES NOT CONTAIN $ [and]
Account Name NOT EQUAL TO NA [and]
Account Name DOES NOT CONTAIN SYSTEM [and]
Account Name NOT EQUAL TO - [and]
Account Name NOT EQUAL TO ANONYMOUS LOGON [and]
Account Name DOES NOT CONTAIN DWM
AND
baseeventid EQUAL TO 4625 [or]
baseeventid EQUAL TO 4771

Directives

Name Abnormal number of logon failures-account
Filter for Events matching criteria? NA
Having similar accountname
Number of Occurrences 5
Within Duration 00:15:00
Should events happen consecutively? false
Distinct? resourcename

Verbose Info
Account ${accountname!"ACCOUNTNAME"} had a spike in failed logins from IP addresses: ${ipaddress$LIST!"UNKNOWN"} Host: ${resourcename$LIST!"UNKNOWN"}

Response Bot Fields/Attributes/Policies
Abnormal number of failed logons from an ipaddress-SIEM-13
Abnormal number of logon failures-SIEM-13
Abnormal number of remote logon attempts-SIEM-13
Abnormal number of failed logons on a resource- SIEM-13
Multiple failed logons
Abnormal number of logon failures
Suspicious Logon Attempts
Abnormal number of remote logon attempt
Rare host accessed by an account - Logon Failure
Abnormal number of remote logon attempts
Abnormal number of failed logons from an ipaddress-SIEM-17
Abnormal number of failed logons on a resource- SIEM-17

Abnormal Number of Logon Failures–SIEM-13
Criticality: Low
Applies to: Functionality
Policy Category: Account Misuse

Device Category
Windows

Description
Abnormal number of logon failures could be indicative of a possible account takeover attempt. Logon failure reason could further indicate the severity of this attack

Technique Used
Behavior anomaly on the logon failure activity for an account

Analytical Type
Directive Based

Prerequisites
- windows logs
- Account naming convention if svc accounts are to be excluded

Violation Entity
Resource Group Account

Threat Focus Area
Cyber

Threat Indicator
Possible bruteforce

Kill Chain Stage
Recon

Remediation Steps

Nessus LaunchScan; NessusConnector StopScan; NessusConnector FetchScan; AD BlockUser; AD UnBlockUser; Tanium - Machine Information; Tanium - Running Processes with MD5; Tanium - Running Applications; Tanium - Non-Approved Established Connections; Tanium - User Sessions

Detection Algorithm

Aggregated Event Analytics

Criteria to Filter Event

Account Name IS NOT NULL [and]
Account Name DOES NOT CONTAIN $ [and]
Account Name DOES NOT CONTAIN svc [and]
Account Name NOT EQUAL TO ANONYMOUS LOGON [and]
Account Name NOT EQUAL TO - [and]
Account Name NOT EQUAL TO NA [and]
Account Name CONTAINS SYSTEM [and]
Account Name DOES NOT CONTAIN Window Manager [and]
Account Name DOES NOT CONTAIN DWM
AND
baseeventid EQUAL TO 4625 [or]
baseeventid EQUAL TO 4771

Directives

Name Abnormal number of logon failures
Filter for Events matching criteria? NA
Having similar accountname
Number of Occurrences 10
Within Duration 00:30:00
Should events happen consecutively? false
Distinct? resourcename

Risk Boosters

Match Criteria:
baseeventid equal to 4625 [or]
baseeventid equal to 4771
Increase factor 1.0

Verbose Info

Account: ${accountname!"ACCOUNTNAME"} IP address: ${ipaddress!"UNKNOWN"} Host: ${resourcename!"UNKNOWN"} Destination User: ${destinationusername!"UNKNOWN"} Message: ${message!"UNKNOWN"} EventID: ${baseeventid!"UNKNOWN"}

Response Bot Fields/Attributes/Policies

Abnormal number of failed logons from an ipaddress-SIEM-13
Abnormal number of kerberos pre authentication failures-SIEM-13
Abnormal number of logon failures from an account-SIEM-13
Abnormal number of failed logons on a resource- SIEM-13
Multiple failed logons
Abnormal number of kerberos pre authentication failures
High number of accounts from the same ipaddress for authentication failures or lockout events
Abnormal number of logon failures
Rare host accessed by an account - Logon Failure
High Number of Failed Logins from an Undocumented Account
Suspicious Account Activity - Peak Credential Validation Failure Increase For Host Analytic

Successful Login after Repeat Failed Login
Abnormal number of failed logons from an ipaddress-SIEM-17
Abnormal number of kerberos pre authentication failures-SIEM-17
Abnormal number of failed logons on a resource- SIEM-17
Abnormal number of failed logins for an account

Abnormal Number of Password Resets

Criticality: Low
Applies to: Functionality
Policy Category: Account Misuse

Device Category

Windows

Description

Abnormal Number of Password Resets

Technique Used

Behavior anomaly on password reset activity

Analytical Type

Tier 2 Behavior Summary

Prerequisites

- windows logs
- Behavior profiles
- user account naming convention
- HR data to identify user roles

Violation Entity

Resource Group Account

Threat Focus Area

Insider/Cyber

Threat Indicator

Possible privilege misuse

Kill Chain Stage

Delivery

Remediation Steps

Possible steps for further analysis/triage to consider:

1. Determine if the activity is approved by:
    - Checking service management system for an incident / work order (ticket) associated with the activity
    - Comparison to the user's peer group
    - Role to privilege comparison
2. Determine if the source account has other anomalies.
3. Determine if the endpoint has other anomalies associated with its processes, sessions, or network connections.

Possible Remediation steps after further analysis and triage:

1. Submit a ticket to reset passwords/disable the account(s).
2. Submit a ticket to remove the account(s) (as needed)
3. Submit a ticket to revoke privileges
4. Submit a ticket to perform a full Antivirus scan
5. Submit a ticket for host isolation and further remediation as per internal IR playbooks dictate.

Notes:

- Domain Admins add/or Desktop Support with User account control privileges on Activity Directory May Trigger this alert from time to time as the amount of password resets is dependent on the user forgetting their passwords.
- Scripts designed to update Service account passwords may also trigger this as well.

Detection Algorithm

Spike in Number of Occurrences

Criteria to Filter Event

baseeventid EQUAL TO 4723 [or]
baseeventid EQUAL TO 4724
AND
Account Name NOT EQUAL TO - [and]
Account Name DOES NOT CONTAIN $ [and]
Account Name DOES NOT CONTAIN ANONYMOUS [and]
Account Name DOES NOT CONTAIN LOCAL

Risk Boosters

Active List:
- Accountname on Suspciious_host_accesse increase factor 4.0
- employeeid on Possible_Bruteforce increase factor 4.0
- employeeid on Suspicious_process_anomaly increase factor 4.0
- employeeid on suspicious_AD_authentication increase factor 4.0
- employeeid on possible_privilege_misuse increase factor 4.0
- employeeid on vulnerable_endpoints increase factor 4.0
- employeeid on infected_endpoints increase factor 4.0

Verbose Info

Account: ${accountname!"ACCOUNTNAME"} IP address: ${ipaddress!"UNKNOWN"} Host: ${resourcename!"UNKNOWN"} Destination User: ${destinationusername!"UNKNOWN"} Message: ${message!"UNKNOWN"} EventID: ${baseeventid!"UNKNOWN"}

Response Bot Fields/Attributes/Policies

Abnormal number of domain password reset attempts-SIEM-13
Abnormal number of password resets-SIEM-13
Password Reset Anomaly
Abnormal number of domain password reset attempts
Abnormal number of domain password reset attempts-SIEM-17

Abnormal Number of Password Resets–SIEM-13

Criticality: Low
Applies to: Functionality
Policy Category: Account Misuse

Device Category

Windows

Description
This may be indicative of a possible account takeover attempt. Unauthorized password changes on multiple accounts could also indicate denial of service.

Technique Used
Behavior anomaly on password reset activity

Analytical Type
Directive Based

Prerequisites
- windows logs
- user account naming convention
- HR data to identify user roles

Violation Entity
Resource Group Account

Threat Focus Area
Insider/Cyber

Threat Indicator
Possible privilege misuse

Kill Chain Stage
Delivery

Remediation Steps
Possible steps for further analysis / triage to consider:

1. Determine if the activity is approved by:
    - Checking service management system for an incident/work order (ticket) associated with the activity
    - Comparison to the user's peer group
    - Role to privilege comparison
2. Determine if the source account has other anomalies.
3. Determine if the endpoint has other anomalies associated with its processes, sessions, or network connections.

Possible Remediation steps after further analysis and triage:

1. Submit a ticket to reset passwords / disable the account(s).
2. Submit a ticket to remove the account(s) (as needed)
3. Submit a ticket to revoke privileges
4. Submit a ticket to perform a full Antivirus scan
5. Submit a ticket for host isolation and further remediation as per internal IR playbooks dictate.

Notes:

- Domain Admins add/or Desktop Support with User account control privileges on Activity Directory May Trigger this alert from time to time as the amount of password resets is dependent on the user forgetting their passwords.
- Scripts designed to update Service account passwords may also trigger this as well.

Detection Algorithm
Aggregated Event Analytics

Criteria to Filter Event

Account Name IS NOT NULL [and]
Account Name DOES NOT CONTAIN svc [and]
baseeventid EQUAL TO 4724 [and]
u_id NOT EQUAL TO -1
AND
Account Name DOES NOT CONTAIN LOCAL [and]
Account Name DOES NOT CONTAIN ANONYMOUS

Directives

Name Abnormal number of password resets
Filter for Events matching criteria? NA
Having similar accountname
Number of Occurrences 20
Within Duration 00:59:59
Should events happen consecutively? false
Distinct? NA

Verbose Info

Account: ${accountname!"ACCOUNTNAME"} IP address: ${ipaddress!"UNKNOWN"} Host: ${resourcename!"UNKNOWN"} Destination User: ${destinationusername!"UNKNOWN"} Message: ${message!"UNKNOWN"} EventID: ${baseeventid!"UNKNOWN"}

Response Bot Fields/Attributes/Policies

Password Reset Anomaly
Abnormal number of password resets
Abnormal number of domain password reset attempts-SIEM-13
Rare password reset for domain admin
Abnormal number of domain password reset attempts
Abnormal number of domain password reset attempts-SIEM-17

Abnormal Number of Privileges Enumerated

Criticality: Low
Applies to: Functionality
Policy Category: Account Misuse

Device Category

Windows

Description

This could indicate a possible LDAP scanning event caused by a malicious presence. Enumeration of privileges is typically leveraged by malwares to achieve privilege escalation

Analytical Type

Tier 2 Behavior Summary

Prerequisites

- windows logs
- Behavior profiles
- user HR dara
- user naming convention

Violation Entity

Resource Group Account

Threat Focus Area

Insider/Cyber

Threat Indicator

Possible privilege misuse

Kill Chain Stage

Exploit

Remediation Steps

Possible steps for further analysis / triage to consider:

1. Determine if the activity is approved by:
    - Checking service management system for an incident / work order (ticket) associated with the activity
    - Comparison to the user's peer group
    - Role to privilege comparison
2. Determine if the target accounts have any anomalies
3. Determine if the source account has other anomalies.
4. Determine if the endpoint has other anomalies associated with its processes, sessions, or network connections.

Possible Remediation steps after further analysis and triage:

1. Submit a ticket to reset passwords / disable the account(s).
2. Submit a ticket to remove the account(s) (as needed)
3. Submit a ticket to revoke privileges
4. Submit a ticket to perform a full Antivirus scan
5. Submit a ticket for host isolation and further remediation as per internal IR playbooks dictate

Note:

- Desktop Support personnel may trigger this event if they need to elevate a user to admin / super user privileges for service management ticket.

Detection Algorithm

Spike in Number of Occurrences

Criteria to Filter Event

baseeventid EQUAL TO 4798 [or]
baseeventid EQUAL TO 4799
AND
Account Name DOES NOT CONTAIN $ [and]
Account Name DOES NOT CONTAIN LOCAL [and]
Account Name DOES NOT CONTAIN ANONYMOUS [and]
Account Name NOT EQUAL TO -

Verbose Info

Account: ${accountname!"ACCOUNTNAME"} IP address: ${ipaddress!"UNKNOWN"} Host: ${resourcename!"UNKNOWN"} Destination User: ${destinationusername!"UNKNOWN"} Message: ${message!"UNKNOWN"} EventID: ${baseeventid!"UNKNOWN"}

Response Bot Fields/Attributes/Policies

Abnormal number of service tickets requested-SIEM-13
Abnormal number of accounts enumerated
Possible AD Enumeration
Rare privilege enumeration event
Abnormal number of account enumeration attempts on an endpoint
Possible Privilege Enumeration

Abnormal Number of Remote Logon Attempts

Criticality: Low
Applies to: Functionality
Policy Category: Account Misuse

Device Category

Windows

Description

This policy detects a spike in successful remote interactive logons which could indicate lateral movement

Analytical Type

Tier 2 Behavior Summary

Prerequisites

- windows logs
- Behavior profiles
- user HR data
- user naming convention
- Host naming convention

Violation Entity

Resource Group Account

Threat Focus Area

Insider/Cyber

Threat Indicator

Suspicious AD Authentication

Kill Chain Stage

Recon

Remediation Steps

Possible steps for further analysis / triage to consider:

1. Determine if the activity is approved by:
    - Checking service management system for an incident / work order (ticket) associated with the activity
    - Comparison to the user's peer group
    - Role to privilege comparison
2. Determine if the target accounts have any anomalies
3. Determine if the source account has other anomalies.
4. Determine if the endpoint has other anomalies associated with its processes, sessions, or network connections.

Possible Remediation steps after further analysis and triage:

1. Submit a ticket to reset passwords / disable the account(s).
2. Submit a ticket to remove the account(s) (as needed)
3. Submit a ticket to revoke privileges
4. Submit a ticket to perform a full Antivirus scan
5. Submit a ticket for host isolation and further remediation as per internal IR playbooks dictate

Note:

- Desktop Support/Network Engineers/Administrators will likely trigger this event from time to time due to need to make changes or login to multiple devices in an environment in a short time. So, verify if this is the case before escalation.

Detection Algorithm

Spike in Number of Occurrences

Criteria to Filter Event

baseeventid EQUAL TO 4624 [or]
baseeventid EQUAL TO 528 [or]
AND
CustomNumber 1 CONTAINS 10 [and]
Account Name DOES NOT CONTAIN $ [and]
Account Name DOES NOT CONTAIN LOCAL [and]
Account Name NOT EQUAL TO - [and]
Account Name DOES NOT CONTAIN ANONYMOUS [and]
Account Name DOES NOT CONTAIN SYSTEM [and]
Account Name NOT EQUAL TO NA [and]
Account Name DOES NOT CONTAIN Window Manager [and]
Account Name DOES NOT CONTAIN DWM

Verbose Info

Account: ${accountname!"ACCOUNTNAME"} IP address: ${ipaddress!"UNKNOWN"} Host: ${resourcename!"UNKNOWN"} Message: ${message!"UNKNOWN"} EventID: ${baseeventid!"UNKNOWN"}

Response Bot Fields/Attributes/Policies

Abnormal number of remote logon attempts-SIEM-13
Abnormal number of remote logon attempt

Abnormal Number of Remote Logon Attempts–SIEM-13

Criticality: Low
Applies to: Functionality
Policy Category: Account Misuse

Device Category

Windows

Description

This policy detects a spike in successful remote interactive logons which could indicate lateral movement

Analytical Type

Directive Based

Prerequisites

- windows logs
- user HR data
- user naming convention
- Host naming convention

Violation Entity

Resource Group Account

Threat Focus Area

Insider/Cyber

Threat Indicator

Suspicious AD Authentication

Kill Chain Stage

Recon

Remediation Steps

Possible steps for further analysis/triage to consider:

1. Determine if the activity is approved by:
2. Checking service management system for an incident / work order (ticket) associated with the activity
3. Comparison to the user's peer group
4. Role to privilege comparison
5. Determine if the target accounts have any anomalies
6. Determine if the source account has other anomalies.
7. Determine if the endpoint has other anomalies associated with its processes, sessions, or network connections.

Possible Remediation steps after further analysis and triage:

1. Submit a ticket to reset passwords/disable the account(s).
2. Submit a ticket to remove the account(s) (as needed)
3. Submit a ticket to revoke privileges
4. Submit a ticket to perform a full Antivirus scan
5. Submit a ticket for host isolation and further remediation as per internal IR playbooks dictate

Note:

- Desktop Support/Network Engineers/Administrators will likely trigger this event from time to time due to need to make changes or login to multiple devices in an environment in a short time. So, verify if this is the case before escalation.

Detection Algorithm

Aggregated event analytics

Criteria to Filter Event

Account Name IS NOT NULL [and]
Account Name DOES NOT CONTAIN $ [and]
Account Name DOES NOT CONTAIN svc [and]
CustomNumber 1 EQUAL TO 10 [and]
Account Name NOT EQUAL TO - [and]
Destination HostName NOT EQUAL TO - [and]
Destination HostName NOT EQUAL TO localhost [and]
Account Name NOT EQUAL TO ANONYMOUS LOGON [and]
Account Name NOT EQUAL TO DWM [and]

Account Name NOT EQUAL TO NA [and]
Account Name DOES NOT CONTAIN SYSTEM [and]
Account Name DOES NOT CONTAIN Window Manager
AND
baseeventid EQUAL TO 528 [or]
baseeventid EQUAL TO 4624

Directives

Name Abnormal number of remote logons
Filter for Events matching criteria? baseeventid CONDITION_EQUALS 4624 AND customnumber1 CONDITION_EQUALS 10
Having similar accountname
Number of Occurrences 5
Within Duration 00:30:00
Should events happen consecutively? false
Distinct? resourcename

Risk Boosters

Match Criteria:
baseenventid equal to 4624 [or]
baseenventid equal to 528
increase factor 2.0

Verbose Info

Account: ${accountname!"ACCOUNTNAME"} IP address: ${ipaddress$LIST!"UNKNOWN"} Host: ${resourcename$LIST!"UNKNOWN"} Message: ${message!"UNKNOWN"} EventID: ${baseeventid!"UNKNOWN"}

Response Bot Fields/Attributes/Policies

Abnormal number of remote interactive logon from an account-SIEM-13
Abnormal number of remote logon attempt
Remote interactive logon to domain controller by non-admin account
Abnormal number of remote logon attempts

Abnormal Number of Run-as Activity–SIEM-13

Criticality: Low
Applies to: Functionality
Policy Category: Account Misuse

Device Category

Windows

Description

Detects remote interactive logins, which is a technique malicious attackers use to laterally move across a network.

Analytical Type

Directive Based

Prerequisites

- windows logs
- user HR data
- user naming convention
- Host naming convention

Violation Entity
Activity Account

Threat Indicator
Suspicious Process execution

Kill Chain Stage
Execute

Remediation Steps
Possible steps for further analysis / triage to consider:

1. Determine if the activity is approved by:
    - Checking service management system for an incident / work order (ticket) associated with the activity
    - Comparison to the user's peer group
    - Role to privilege comparison
2. Determine if the target accounts have any anomalies
3. Determine if the source account has other anomalies.
4. Determine if the endpoint has other anomalies associated with its processes, sessions, or network connections.

Possible Remediation steps after further analysis and triage:

1. Submit a ticket to reset passwords/disable the account(s).
2. Submit a ticket to remove the account(s) (as needed)
3. Submit a ticket to revoke privileges
4. Submit a ticket to perform a full Antivirus scan
5. Submit a ticket for host isolation and further remediation as per internal IR playbooks dictate

Note:

- Desktop Support personnel commonly use "Run As" to execute tasks while completing service tickets.
- Service accounts generally carry out batch jobs that may also trigger this event from time to time.

Detection Algorithm
Aggregated event analytics

Criteria to Filter Event
Account Name DOES NOT CONTAIN $ [and]
Account Name IS NOT NULL [and]
baseeventid EQUAL TO 4648 [and]
Account Name DOES NOT CONTAIN svc [and]
Account Name NOT EQUAL TO - [and]
Account Name DOES NOT CONTAIN LOCAL [and]
Account Name DOES NOT CONTAIN ANONYMOUS

Directives
Name Abnormal number of run-as activity
Filter for Events matching criteria? NA
Having similar accountname
Number of Occurrences 50
Within Duration 00:59:59
Should events happen consecutively? false
Distinct? NA

Verbose Info
Account: ${accountname!"ACCOUNTNAME"} IP address: ${ipaddress!"UNKNOWN"} Host: ${resourcename!"UNKNOWN"} Destination User: ${destinationusername!"UNKNOWN"} Message: ${message!"UNKNOWN"} EventID: ${baseeventid!"UNKNOWN"}

Response Bot Fields/Attributes/Policies
High number of accounts used on a workstation for successful authentications or run as events
High number of accounts from the same ipaddress for successful authentications or run as events
Use of explicit credentials - Account sharing or Password misuse
Abnormal number of process execution using explicit credentials
Rare target account authentication using explicit credentials
Rare process detected for authentication using explicit credentials
Suspicious Account Activity - Peak Explicit Credentials Distinct Account Name For Host Analytic

---

Abnormal Number of Service Tickets Requested–SIEM-13
Criticality: Low
Applies to: Functionality
Policy Category: Account Misuse

Device Category
Windows

Description
Abnormal number of server access requests

Analytical Type
Directive Based

Prerequisites
- windows logs
- Account Naming conventions
- Host naming conventions

Violation Entity
Resource Group Account

Threat Indicator
Suspicious Network Share Access

Kill Chain Stage
Recon

Remediation Steps
Possible steps for further analysis/triage to consider:

1. Determine if the referenced Service Account (Resource, if listed) has any anomalies.
2. Determine if the account has other anomalies.
3. Determine if the endpoint has other anomalies associated with its processes, sessions, or network connections.

Possible Remediation steps after further analysis and triage:

1. Submit a ticket to reset the service account password.
2. Submit a ticket to disable the source account or service account (as needed).
3. Submit a ticket to scan host for vulnerabilities &/or malware (as needed).
4. Open an investigation as per internal IR playbook dictates.

Detection Algorithm
Aggregated event analytics

Criteria to Filter Event
baseeventid EQUAL TO 4769 [and]
Account Name IS NOT NULL [and]
Account Name NOT EQUAL TO - [and]
Account Name NOT EQUAL TO krbtgt [and]
Account Name DOES NOT CONTAIN sql [and]
Account Name DOES NOT CONTAIN svc [and]
Account Name DOES NOT CONTAIN SPFarm [and]
Account Name DOES NOT CONTAIN SPSearch [and]
Account Name DOES NOT CONTAIN $ [and]
filepath DOES NOT CONTAIN LAN ID [and]
Source HostName DOES NOT START WITH ADS [and]
filepath DOES NOT CONTAIN krbtgt

Directives
Name ServiceTicketRequest
Filter for Events matching criteria? baseeventid CONDITION_EQUALS 4769
Having similar accountname
Number of Occurrences 7
Within Duration 00:05:00
Should events happen consecutively? false
Distinct? filepath

Verbose Info
Account: ${accountname!"ACCOUNTNAME"} IP address: ${ipaddress!"UNKNOWN"} Host: ${resourcename!"UNKNOWN"} Destination User: ${destinationusername!"UNKNOWN"} Message: ${message!"UNKNOWN"} EventID: ${baseeventid!"UNKNOWN"}

Response Bot Fields/Attributes/Policies
Abnormal number of Kerberos impersonation attempts detected -13
Abnormal number of Kerberos pre authentication failures-SIEM-13
Abnormal number of Kerberos pre authentication failures
Suspicious Account Activity - Kerberoasting - Peak TGS Request For User Analytic
Abnormal number of Kerberos impersonation attempts detected -17
Abnormal number of Kerberos pre authentication failures-SIEM-17

Abnormal Number of Successful Authentication Attempts
Criticality: Low
Applies to: Functionality
Policy Category: Account Misuse

Device Category
Windows

Description
A spike in the number of successful logins for a user account can indicate account misuse through password/account sharing, which as a best practice is a corporate policy violation or lateral movement if there are many remote interactive logins

Analytical Type
Tier 2 Behavior Summary

Prerequisites
- windows logs
- User Behavior profiles
- User naming conventions to identify users that may carryout

Violation Entity
Resource Group Account

Threat Focus Area
Insider/Cyber

Threat Indicator
Suspicious AD Authentication

Kill Chain Stage
Recon

Remediation Steps
Possible steps for further analysis/triage to consider:

1. Determine if the activity is approved by:
    - Checking service management system for an incident / work order (ticket) associated with the activity
    - Comparison to the user's peer group
    - Role to privilege comparison
2. Determine if the account has other anomalies.
3. Determine if the endpoint has other anomalies associated with its processes, sessions, or network connections.

Possible Remediation steps after further analysis and triage:

1. Submit a ticket to reset password/disable the account.
2. Submit a ticket to remove the account (as needed)
3. Submit a ticket to revoke privileges

Notes:

- If a service account observed validate activity is approved and add the account to whitelist or update use case criteria to exclude

Detection Algorithm
Spike in Number of Occurrences

Criteria to Filter Event
baseeventid EQUAL TO 4624 [or]
baseeventid EQUAL TO 528 [or]
Account Name EQUAL TO 540
AND
Account Name DOES NOT CONTAIN svc [and]
Account Name DOES NOT CONTAIN DWM [and]
Account Name NOT EQUAL TO Anonymous Logon [and]
Account Name DOES NOT CONTAIN $ [and]
Account Name NOT EQUAL TO NA [and]
Account Name NOT EQUAL TO - [and]
Account Name DOES NOT CONTAIN Window Manager [and]
Account Name DOES NOT CONTAIN SYSTEM

Verbose Info
Account: ${accountname!"ACCOUNTNAME"} IP address: ${ipaddress!"UNKNOWN"} Host: ${resourcename!"UNKNOWN"} Destination User: ${destinationusername!"UNKNOWN"} Message: ${message!"UNKNOWN"} EventID: ${baseeventid!"UNKNOWN"}

Response Bot Fields/Attributes/Policies
High number of accounts used on a workstation for successful authentications or run as events
High number of accounts from the same ipaddress for successful authentications or run as events

---

Abnormal Object or Network Share Access Attempts–SIEM-13
Criticality: High
Applies to: Functionality
Policy Category: Account Misuse

Device Category
Windows

Description
A spike in account accessing new network objects may be indicative of a possible snooping or a recon activity

Technique Used
Behavior anomaly on the network share access activity

Analytical Type
Directive Based

Prerequisites
- windows logs
- User naming convention

Violation Entity
Resource Group Account

Threat Focus Area
Insider/Cyber

Threat Indicator
Suspicious Network Share Access

Kill Chain Stage
Recon

Remediation Steps
Possible steps for further analysis/triage to consider:

1. Determine if the activity is approved by:
    - Checking service management system for an incident / work order (ticket) associated with the activity
    - Comparison to the user's peer group
    - Role to privilege comparison
2. Determine if the source account has other anomalies.
3. Determine if the endpoint has other anomalies associated with its processes, sessions, or network connections.

Possible Remediation steps after further analysis and triage:

1. Submit a ticket to revert any changes that occurred.
2. Submit a ticket to reset passwords / disable the account(s).
3. Submit a ticket to remove the account(s) (as needed)
4. Submit a ticket to revoke privileges
5. Submit a ticket to perform a full Antivirus scan
6. Submit a ticket for host isolation and further remediation as per internal IR playbooks dictate.

Detection Algorithm

Aggregated event analytics

Criteria to Filter Event

Account Name IS NOT NULL [and]
baseeventid EQUAL TO 5140 [and]
Account Name DOES NOT CONTAIN $ [and]
Account Name DOES NOT CONTAIN LOCAL [and]
Account Name DOES NOT CONTAIN svc [and]
Source HostName DOES NOT CONTAIN ADC [and]
Source HostName DOES NOT CONTAIN ADS [and]
Account Name NOT EQUAL TO - [and]
Account Name DOES NOT CONTAIN ANONYMOUS

Directives

Name Abnormal object or network share access attempts
Filter for Events matching criteria? baseeventid CONDITION_EQUALS 5140
Having similar accountname
Number of Occurrences 5
Within Duration 00:30:00
Should events happen consecutively? false
Distinct? sourcehostname

Risk Boosters

Match criteria:
baseeventid equal to 5140 increase factor 5.0

Verbose Info

Account: ${accountname!"ACCOUNTNAME"} IP address: ${ipaddress!"UNKNOWN"} Host: ${resourcename$LIST!"UNKNOWN"} Share Name: ${resourcecustomfield5$LIST!"UNKNOWN"} Message: ${message!"UNKNOWN"} EventID: ${baseeventid!"UNKNOWN"}

Response Bot Fields/Attributes/Policies

Rare host accessed by an account
Abnormal number of host access attempts
Rare host accessed by an account - Logon Success
Rare host accessed by an account - Logon Failure
Rare Host Accessed Attempt by Account
Rare Host Accessed from an Account
Suspicious host access behavior from an account
Abnormal number of administrative share object accessed-SIEM-17
Unusual high number of network shares accessed – SIEM
Spike in administrative shares accessed
Abnormal number of administrative share object accessed
Abnormal number of network share object access
Rare admin share access by an account
Abnormal number of administrative share object accessed-SIEM-13

Abnormal object or network share access attempts by resource-SIEM-13

Account Added and Removed to Security Group

Criticality: Medium
Applies to: Functionality
Policy Category: Account Misuse

Device Category

Windows

Description

These temporary privilege escalation events may be indicative of a possible backdoor access attempt to use elevated privileges

Technique Used

Entity attribution

Analytical Type

Directive Based

Prerequisites

- windows logs
- Account naming convention

Violation Entity

Activity Account

Threat Focus Area

Insider/Cyber

Threat Indicator

Possible Escalation of Privileges

Kill Chain Stage

Recon

Remediation Steps

Possible steps for further analysis/triage to consider:

1. Determine if the escalated account has other anomalies
2. Determine if the Source account has other anomalies.
3. Determine if the account should be performing the activity via a role to privilege comparison.

Possible Remediation steps after further analysis and triage:

1. Submit a ticket to revert any changes that occurred.
2. Submit a ticket to reset password/disable the account(s).
3. Submit a ticket to remove the account(s) (as needed)
4. Submit a ticket to revoke privileges

Criteria to Filter Event

baseeventid EQUAL TO 4728 [or]
baseeventid EQUAL TO 4729 [or]
baseeventid EQUAL TO 4732 [or]

baseeventid EQUAL TO 4756 [or]
baseeventid EQUAL TO 4733 [or]
baseeventid EQUAL TO 4757
AND
Destination User Name IS NOT NULL
Source User Privileges IS NOT NULL [and]
Destination User Name NOT EQUAL TO - [and]
Source User Privileges NOT EQUAL TO -

Directives

Parent
Name Member added
Filter for Events matching criteria? baseeventid CONDITION_EQUALS 4728 OR
baseeventid CONDITION_EQUALS 4732 OR
baseeventid CONDITION_EQUALS 4756
Having similar accountname,destinationusername,destinationuserprivileges
Number of Occurrences 1
Within Duration 06:00:00
Should events happen consecutively? false
Distinct? NA

Child
Name Member Removed
Filter for Events matching criteria? baseeventid CONDITION_EQUALS 4729 OR
baseeventid CONDITION_EQUALS 4733 OR
baseeventid CONDITION_EQUALS 4757
Number of Occurrences 1
Within Duration 06:00:00
Should events happen consecutively? false
Distinct? NA
Minimum duration between parent and child 06:00:00
Common between parent and child?
accountname,destinationusername,destinationuserprivileges,devicecustomstring1

Risk Boosters

Active list:
employeeid on:
Suspicious_host_accessed
possible_bruteforce
suspicious_process_anomali
suspicious_AD_authentication
vulnerable_endpoints
infected_endpoints
increase factor 4.0

Verbose Info

Account ${accountname!"unknown"} performed a possible privilege escalation by adding and removing the account ${destinationuser!"UNKNOWN"} to the group ${sourceuserprivileges!"UNKNOWN"}

Response Bot Fields/Attributes/Policies

A member was added and removed from a security enabled group within a short time-13
A member was added and removed from a security enabled group within a short time-17

Account Created and Deleted

Criticality: Medium

Applies to: Functionality
Policy Category: Account Misuse

Device Category
Windows

Description
Temporarily creating and deleting an account may be indicative of a possible backdoor access attempt to use elevated privileges

Technique Used
Entity attribution

Analytical Type
Directive Based

Prerequisites
- windows logs
- HR Data
- User Data

Violation Entity
Activity Account

Threat Focus Area
Cyber

Threat Indicator
Possible backdoor account

Kill Chain Stage
Exploit

Remediation Steps
Possible steps for further analysis / triage to consider:

1. Determine if the activity is approved by:
    - Checking service management system for an incident / work order (ticket) associated with the activity
    - Comparison to the user's peer group
    - Role to privilege comparison
2. Determine if the created account activities are anomalies or expected.
3. Determine if the source account has other anomalies.
4. Determine if the endpoint has other anomalies associated with its processes, sessions, or network connections.

Possible Remediation steps after further analysis and triage:

1. Submit a ticket to revert any changes made.
2. Submit a ticket to reset password / disable the source account.
3. Submit a ticket to remove the account (as needed)
4. Submit a ticket to revoke privileges

Notes:

- Domain Admins may create and delete users as part of troubleshooting steps.

Criteria to Filter Event

baseeventid equal to 624 [or]
baseeventid EQUAL TO 4720 [or]
baseeventid EQUAL TO 4726 [or]
baseeventid EQUAL TO 624 [or]
baseeventid EQUAL TO 630

Directives

Parent
Name Account Created
Filter for Events matching criteria? eventid CONDITION_EQUALS 4720
Having similar accountname,destinationusername
Number of Occurrences 1
Within Duration 06:00:00
Should events happen consecutively? false
Distinct? NA

Child
Name Account Deleted
Filter for Events matching criteria? eventid CONDITION_EQUALS 4726
Number of Occurrences 1
Within Duration 06:00:00
Should events happen consecutively? false
Distinct? NA
Minimum duration between parent and child 06:00:00
Common between parent and child? accountname,destinationusername

Risk Boosters

Active List:
accountname in:
- suspicious_host_accessed
- possible_bruteforce
- suspicious process_anomaly
- suspicious_AD_authentication
- possible_privilege_misuse
- vulnerable_endpoints
- infected_endpoints
increase factor 4.0

Verbose Info

Account ${accountname!"ACCOUNTNAME"} was detected creatng and deleting ${destinationusername!"Target"} from ipaddress ${ipaddress!"UNKNOWN"}

Response Bot Fields/Attributes/Policies

Account Enabled and Disabled
Abnormal number of account creation-disabled

Account Enabled and Disabled

Criticality: Medium
Applies to: Functionality
Policy Category: Account Misuse

Device Category

Windows

Description
Temporarily enabling and disabling an account may be indicative of a possible backdoor access attempt to use elevated privileges

Technique Used
Entity attribution

Analytical Type
Directive Based

Prerequisites
- windows logs
- HR Data
- User Data

Violation Entity
Activity Account

Threat Focus Area
Insider/Cyber

Threat Indicator
Possible Escalation of Privileges

Kill Chain Stage
Recon

Remediation Steps
Possible steps for further analysis / triage to consider:

1. Determine if the activity is approved by:
    - Checking service management system for an incident / work order (ticket) associated with the activity
    - Comparison to the user's peer group
    - Role to privilege comparison
2. Determine if the target account activities are anomalies or expected.
3. Determine if the source account has other anomalies.
4. Determine if the endpoint has other anomalies associated with its processes, sessions, or network connections.

Possible Remediation steps after further analysis and triage:

1. Submit a ticket to revert any changes made.
2. Submit a ticket to reset password / disable the source account.
3. Submit a ticket to remove the account (as needed)
4. Submit a ticket to revoke privileges

Criteria to Filter Event
baseeventid EQUAL TO 4722 [or]
baseeventid EQUAL TO 4725

Directives
Parent

Name Account Enabled
Filter for Events matching criteria? baseeventid CONDITION_EQUALS 4722
Having similar accountname,destinationusername,destinationuserprivileges
Number of Occurrences 1
Within Duration 06:00:00
Should events happen consecutively? false
Distinct? NA

Child
Name Account Disabled
Filter for Events matching criteria? baseeventid CONDITION_EQUALS 4725
Number of Occurrences 1
Within Duration 06:00:00
Should events happen consecutively? false
Distinct? NA
Minimum duration between parent and child 00:02:00
Common between parent and child? accountname,destinationusername,destinationuserprivileges

Risk Boosters

Active List:
accountname in suspicious_host_accessed [and/or]
employeeid in:
- possible_bruteforce
- suspicious process_anomaly
- suspicious_AD_authentication
- possible_privilege_misuse
- vulnerable_endpoints
- infected_endpoints
increase factor 4.0

Verbose Info

Account ${accountname!"ACCOUNTNAME"} was detected enabling ${destinationusername!"ACTIVITY"} and disabling it from ipaddress ${ipaddress!"UNKNOWN"}

Response Bot Fields/Attributes/Policies

Windows activity by terminated accounts
Use of any default credentials

Audit Log Tampering

Criticality: Low
Applies to: Functionality
Policy Category: Account Misuse

Device Category

Windows

Description

Audit log tampering may be an attempt by a malicious entity to clear tracks involving unauthorized activity.

Technique Used

Entity Attribution

Analytical Type

Real Time Policy

Prerequisites
- windows logs
- HR Data
- User naming convention

Violation Entity
Resource Group Account

Threat Focus Area
Insider/Cyber

Threat Indicator
Audit log tampering

Kill Chain Stage
Exploit

Remediation Steps
Possible steps for further analysis / triage to consider:

1. Determine if the activity is approved by:
    - Checking service management system for an incident / work order (ticket) associated with the activity
    - Comparison to the user's peer group
    - Role to privilege comparison
2. Determine if the account's activities were malicious
3. Determine if the endpoint has other anomalies associated with its processes, sessions, or network connections.

Possible Remediation steps after further analysis and triage:

1. Submit a ticket to revert any changes made.
2. Submit a ticket to reset password / disable the source account.
3. Submit a ticket to remove the account (as needed)
4. Submit a ticket to revoke privileges
5. Submit a ticket to isolate host per internal IR Playbook

Note:

- If Best practice of having the log overwrite the oldest events to prevent from filling up, may lead to a Desktop Support user clearing the log check for a service ticket to confirm.

Detection Algorithm
Individual Event Analytics

Criteria to Filter Event
baseeventid EQUAL TO 1102 [and]
message CONTAINS audit
AND
Account Name NOT EQUAL TO - [and]
Account Name DOES NOT CONTAIN LOCAL [and]
Account Name DOES NOT CONTAIN ANONYMOUS [and]
Account Name DOES NOT CONTAIN $ [and]
Account Name DOES NOT CONTAIN system

Risk Boosters
Active List:
accountname in Possible_bruteforce [and/or]
employeeid in:
- suspicious_host_accessed
- suspicious_process_anomaly
- suspicious_AD_authentication
- possible_privilege_misuse
- vulnerable_endpoints
- infected_endpoints
increase factor 4.0

Verbose Info
Account: ${accountname!"ACCOUNTNAME"} IP address: ${ipaddress!"UNKNOWN"} Host: ${resourcename!"UNKNOWN"} Message: ${message!"UNKNOWN"} EventID: ${baseeventid!"UNKNOWN"}

Response Bot Fields/Attributes/Policies
Rare audit log clearing by an account
Audit policy changes
Firewall disabled on windows
Firewall configurations modified on windows
Rare regedit usage compared to peer
Suspicious Registry Modification Observed
Rare registry modification by an account
Suspicious AD policy change

Detection of Domain Trust Additions–Peer Anomaly
Criticality: Low
Applies to: Functionality
Policy Category: Account Misuse

Device Category
Windows

Description
Unauthorized trust additions on a domain may be indicative of a possible privilege abuse and could lead to unauthorized access to services and resources

Technique Used
Behavior anomaly on domain trust additions

Analytical Type
Tier 2 Behavior Summary

Prerequisites
- windows logs
- Behavior profiles

Violation Entity
Activity Account

Threat Focus Area
Insider/Cyber

Threat Indicator
Possible privilege misuse

Kill Chain Stage
Delivery

Remediation Steps
AD BlockUser; AD UnBlockUser; Tanium - Machine Information; Tanium - Running Applications; Tanium - Non-Approved Established Connections

Detection Algorithm
Abnormal Activity Compared to peers

Criteria to Filter Event
baseeventid EQUAL TO 610 [or]
baseeventid EQUAL TO 4716
AND
Account Name NOT EQUAL TO - [and]
Account Name DOES NOT CONTAIN $ [and]
Account Name DOES NOT CONTAIN ANONYMOUS [and]
Account Name DOES NOT CONTAIN LOCAL

Risk Boosters
Active List:
accountname in suspicious_host_accessed [and/or]
employeeid in:
- Possibe_Bruteforce
- suspicious_process_anomaly
- suspicious_AD_authentication
- possible_privilege_misuse
- vulnerable_endpoints
- infected_endpoints
increase factor 4.0

Verbose Info
Account: ${accountname!"ACCOUNTNAME"} IP address: ${ipaddress!"UNKNOWN"} Host: ${resourcename!"UNKNOWN"} Destination User: ${destinationusername!"UNKNOWN"} Message: ${message!"UNKNOWN"} EventID: ${baseeventid!"UNKNOWN"}

Response Bot Fields/Attributes/Policies
Abnormal number of domain password reset attempts-SIEM-13
Abnormal number of run-as activity-SIEM-13
Abnormal number of account creation-SIEM-13
Local accounts created on windows - Target domain analysis
Use of explicit credentials - Account sharing or Password misuse
Firewall disabled on windows
Password Reset Anomaly
Rare audit log clearing by an account
Rare registry modification by an account
Rare regedit usage compared to peer
Password hash access
Suspicious Service creation

Rare service created on endpoint
Rare Basic Service Operation
Rare local account created
Audit Log Tampering
Use of credential dumpers
Detection of possible backdoor
Rare privileged level for windows authentication
Firewall configurations modified on windows
Rare builtin member group additions
Audit policy changes
Restricted Group Change
Suspicious Process Activity - Log Clearing Analytics
Suspicious AD policy change
Scheduled Task Creation
Local accounts created on windows

Domain Account Creation by Users

Criticality: Low
Applies to: Functionality
Policy Category: Account Misuse

Device Category

Windows

Description

Detects a normal user creating a domain account that could indicate an attacker creating and account to use directly.

Analytical Type

Real Time Policy

Prerequisites

- windows logs
- User naming convention
- Host naming Convention

Violation Entity

Resource Group Account

Threat Focus Area

Insider/Cyber

Threat Indicator

Possible privilege misuse

Kill Chain Stage

Delivery

Remediation Steps

Possible steps for further analysis / triage to consider:

1. Determine if the activity is approved by:
    - Checking service management system for an incident / work order (ticket) associated with the activity

- Comparison to the user's peer group
- Role to privilege comparison

2. Determine if the account has other anomalies
3. Determine if the host has other anomalies

Possible Remediation steps after further analysis and triage:

1. Submit a ticket to reset password / disable the source account.
2. Submit a ticket to revoke privileges
3. Submit a ticket to isolate host and execute internal IR Playbook

Detection Algorithm

Individual Event Analytics

Criteria to Filter Event

baseeventid EQUAL TO 4720 [or]
baseeventid EQUAL TO 626
AND
user id not equal to -1
AND
resourcename contains LDAP

Verbose Info

Account: ${accountname!"ACCOUNTNAME"} IP address: ${ipaddress!"UNKNOWN"} Host: ${resourcename!"UNKNOWN"} Destination User: ${destinationusername!"UNKNOWN"} Message: ${message!"UNKNOWN"} EventID: ${baseeventid!"UNKNOWN"}

Response Bot Fields/Attributes/Policies

Abnormal number of account creation-SIEM-13
Abnormal number of password resets-SIEM-13
Firewall disabled on windows
Password Reset Anomaly
Rare audit log clearing by an account
Rare registry modification by an account
Detection of Domain Trust Additions - Peer anomaly
Abnormal number of password resets
Abnormal number of account creation
Rare regedit usage compared to peer
Password hash access
Suspicious Service creation
Rare service created on endpoint
Rare Basic Service Operation
Use of credential dumpers
Rare privileged level for windows authentication
Firewall configurations modified on windows
Rare builtin member group additions
Audit policy changes
Restricted Group Change
Suspicious AD policy change
Suspicious executables on a machine
Scheduled Task Creation

Firewall Configurations Modified on Windows

Criticality: Low
Applies to: Functionality
Policy Category: Account Misuse

Device Category
Windows

Description
Modifying firewall configurations on an endpoint can cause a host to be vulnerable to exploits. It could also indicate a malicious entity attempting to disable firewall.

Technique Used
Entity Attribution

Analytical Type
Real Time Policy

Prerequisites
- windows logs
- Proxy / Firewall Logs
- IP attribution

Violation Entity
Activity Account

Threat Focus Area
Insider/Cyber

Threat Indicator
Circumvention of controls

Kill Chain Stage
Recon

Remediation Steps
VirusTotal ScanIP; VirusTotal ScanURL; VirusTotal ScanDomain; Nessus LaunchScan; NessusConnector StopScan; NessusConnector FetchScan; AD BlockUser; AD UnBlockUser; Tanium - Machine Information; Tanium - Running Processes with MD5; Tanium - Running Applciations; Tanium - Non-approved Established Connections; PassiveTotal - Get Passive DNS; PassiveTotal - Get Subdomains
- PassiveTotal - Get Unique DNS
- PassiveTotal - Get Who Is

Detection Algorithm
Individual Event Analytics

Criteria to Filter Event
baseeventid EQUAL TO 4954 [or]
baseeventid EQUAL TO 4946 [or]
baseeventid EQUAL TO 4947 [or]
baseeventid EQUAL TO 4950

Risk Boosters
Active List:
accountname in suspicious_host_accessed [and/or]
employeeid in:
- Possibe_Bruteforce

- suspicious_process_anomaly
- suspicious_AD_authentication
- possible_privilege_misuse
- vulnerable_endpoints
- infected_endpoints
increase factor 4.0

Verbose Info
Account: ${accountname!"ACCOUNTNAME"} IP address: ${ipaddress!"UNKNOWN"} Host: ${resourcename!"UNKNOWN"} Destination User: ${destinationusername!"UNKNOWN"} Message: ${message!"UNKNOWN"} EventID: ${baseeventid!"UNKNOWN"}

Response Bot Fields/Attributes/Policies
Firewall disabled on windows
Rare regedit usage compared to peer
Rare process creation on an endpoint
Suspicious Service creation
Rare service created on endpoint
Rare token elevation for process
Detection of possible backdoor
Use of credential dumpers
Rare process spawned by a parent process
Audit policy changes
Suspicious Registry Modification Observed
Suspicious Process Activity - Log Clearing Analytics
Suspicious Process Activity - Potential Mimikatz or Hash Passing Token Creation - Powershell Privileged Service Call Analytic
Suspicious Process Activity - Endpoint - Potential Mimikatz Object Handling Activity Analytic
Suspicious AD policy change
Scheduled Task Creation
Audit Log Tampering
Rare audit log clearing by an account

Firewall Disabled on Windows
Criticality: Low
Applies to: Functionality
Policy Category: Account Misuse

Device Category
Windows

Description
Disabling firewall on an endpoint can cause a host to be vulnerable to exploits. It could also indicate a malicious entity attempting to disable firewall.

Technique Used
Entity Attribution

Analytical Type
Real Time Policy

Prerequisites
- windows logs

Violation Entity
Activity Account

Threat Focus Area
Cyber

Threat Indicator
Vulnerable Endpoint

Kill Chain Stage
Recon

Remediation Steps
- Nessus LaunchScan
- NessusConnector StopScan
- NessusConnector FetchScan
- AD BlockUser
- AD UnBlockUser
- Tanium - Machine Information
- Tanium - Running Processes with MD5
- Tanium - Running Applications
- Tanium - Non-approved Established Connections

Detection Algorithm
Individual Event Analytics

Criteria to Filter Event
baseeventid EQUAL TO 5025 [or]
baseeventid EQUAL TO 5034
AND
deviceseverity EQUAL TO OFF [and]
baseeventid EQUAL TO 853

Risk Boosters
Active List:
accountname in suspicious_host_accessed [and/or]
employeeid in:
- suspicious_host_accessed
- suspicious_process_anomaly
- suspicious_AD_authentication
- possible_privilege_misuse
- vulnerable_endpoints
- infected_endpoints

increase factor 4.0

Verbose Info
Account: ${accountname!"ACCOUNTNAME"} IP address: ${ipaddress!"UNKNOWN"} Host: ${resourcename!"UNKNOWN"} Destination User: ${destinationusername!"UNKNOWN"} Message: ${message!"UNKNOWN"} EventID: ${baseeventid!"UNKNOWN"}

Response Bot Fields/Attributes/Policies
Firewall configurations modified on windows
Suspicious Process Activity - Log Clearing Analytics
Suspicious Process Activity - Potential Mimikatz or Hash Passing Token Creation - Powershell Privileged Service Call Analytic
Suspicious Process Activity - Endpoint - Potential Mimikatz Object Handling Activity Analytic
Suspicious AD policy change
Suspicious executables on a machine
Scheduled Task Creation
Rare object access attempts by an account
Detection of possible backdoor
Use of credential dumpers
Audit Log Tampering
Rare token elevation for process
Rare process creation on an endpoint
Suspicious Service creation
Rare regedit usage compared to peer
Rare registry modification by an account
Rare audit log clearing by an account

High Number of Failed Logins from an Undocumented Account
Criticality: Low
Applies to: Functionality
Policy Category: Account Misuse

Device Category
Windows

Description
This may be indicative of a privilege misuse activity

Analytical Type
Real Time Policy

Prerequisites
- windows logs

Violation Entity
Activity Account

Threat Focus Area
Cyber

Threat Indicator
Possible bruteforce

Kill Chain Stage
Recon

Remediation Steps
- Nessus LaunchScan
- NessusConnector StopScan
- NessusConnector FetchScan

- AD BlockUser
- AD UnBlockUser
- Tanium - Machine Information
- Tanium - Running Processes with MD5
- Tanium - Running Applciations
- Tanium - Non-approved Established Connections

Detection Algorithm
Spotter

Criteria to Filter Event
resourcegroupname = "Microsoft Windows Events" and baseeventid=4625 and status!=1 and (accountname=m OR accountname=PC)

Verbose Info
Account: ${accountname!"ACCOUNTNAME"} IP address: ${ipaddress!"UNKNOWN"} Host: ${resourcename!"UNKNOWN"} Destination User: ${destinationusername!"UNKNOWN"} Message: ${message!"UNKNOWN"} EventID: ${baseeventid!"UNKNOWN"}

Response Bot Fields/Attributes/Policies
Abnormal number of remote interactive logon from an account-SIEM-13
Abnormal number of logon failures-SIEM-13
Abnormal number of remote logon attempts-SIEM-13
Abnormal number of logon failures from an account-SIEM-13
Abnormal number of failed logons on a resource- SIEM-13
Multiple failed logons
Abnormal number of logon failures
Suspicious Logon Attempts
Abnormal number of remote logon attempt
Abnormal number of remote logon attempts
Abnormal number of failed logons from an ipaddress-SIEM-17
Abnormal number of failed logons on a resource- SIEM-17

Local Accounts Created on Windows
Criticality: Medium
Applies to: Functionality
Policy Category: Account Misuse

Device Category
Windows

Description
Locally created accounts can't be monitored by the Domain Controller and can be leveraged to avoid defense mechanisms or create backdoors for future malicious use.

Technique Used
Entity Attribution

Analytical Type
Real Time Policy

Prerequisites
- windows logs

Violation Entity
Resource Group Account

Threat Focus Area
Insider/Cyber

Threat Indicator
Circumvention of controls

Kill Chain Stage
Recon

Remediation Steps
- VirusTotal ScanIP
- VirusTotal ScanURL
- VirusTotal ScanDomain
- Nessus LaunchScan
- NessusConnector StopScan
- NessusConnector FetchScan
- AD BlockUser
- AD UnBlockUser
- Tanium - Machine Information
- Tanium - Running Processes with MD5
- Tanium - Running Applciations
- Tanium - Non-approved Established Connections
- PassiveTotal - Get Passive DNS
- PassiveTotal - Get Subdomains
- PassiveTotal - Get Unique DNS
- PassiveTotal - Get Who Is
- PassiveTotal - Search Who is
- PassiveTotal - Search Who is by Keyword

Detection Algorithm
Individual Event Analytics

Criteria to Filter Event
baseeventid EQUAL TO 4720 [or]
baseeventid EQUAL TO 624
AND
Source HostName CONTAINS Destination Network Domain [or]
Destination Network Domain CONTAINS Source HostName
AND
Account Name NOT EQUAL TO - [and]
Account Name DOES NOT CONTAIN $ [and]
Account Name DOES NOT CONTAIN ANONYMOUS [and]
Account Name DOES NOT CONTAIN LOCAL [and]
Destination Network Domain DOES NOT CONTAIN PROD

Risk Boosters
Active List:
accountname in suspicious_host_accessed [and/or]
employeeid in:
- Possible_bruteforce
- suspicious_host_accessed
- suspicious_process_anomaly

- suspicious_AD_authentication
- possible_privilege_misuse
- vulnerable_endpoints
- infected_endpoints
increase factor 4.0

Verbose Info

Account: ${accountname!"ACCOUNTNAME"} IP address: ${ipaddress!"UNKNOWN"} Host: ${resourcename!"UNKNOWN"} Destination User: ${destinationusername!"UNKNOWN"} Account Domain: ${destinationntdomain!"UNKNOWN"} Message: ${message!"UNKNOWN"} EventID: ${baseeventid!"UNKNOWN"}

Response Bot Fields/Attributes/Policies

Account Created and Deleted-13
Abnormal number of account creation-SIEM-13
Account Created and Deleted
Local accounts created on windows - Target domain analysis
Abnormal number of account creation
Rare local account created
Abnormal number of account creation-disabled
Possible local account created

Local Accounts Created on Windows–Target Domain Analysis

Criticality: Medium
Applies to: Functionality
Policy Category: Account Misuse

Device Category

Windows

Description

Locally created accounts can't be monitored by the Domain Controller and can be leveraged to avoid defense mechanisms or create backdoors for future malicious use.

Technique Used

Entity Attribution

Analytical Type

Real Time Policy

Prerequisites

- windows logs

Violation Entity

Resource Group Account

Threat Focus Area

Insider/Cyber

Threat Indicator

Circumvention of controls

Kill Chain Stage
Recon

Remediation Steps
- VirusTotal ScanIP
- VirusTotal ScanURL
- VirusTotal ScanDomain
- Nessus LaunchScan
- NessusConnector StopScan
- NessusConnector FetchScan
- AD BlockUser
- AD UnBlockUser
- Tanium - Machine Information
- Tanium - Running Processes with MD5
- Tanium - Running Applciations
- Tanium - Non-approved Established Connections
- PassiveTotal - Get Passive DNS
- PassiveTotal - Get Subdomains
- PassiveTotal - Get Unique DNS
- PassiveTotal - Get Who Is
- PassiveTotal - Search Who is
- PassiveTotal - Search Who is by Keyword

Detection Algorithm
Individual Event Analytics

Criteria to Filter Event
baseeventid EQUAL TO 4720 [or]
baseeventid EQUAL TO 624
AND
Source HostName CONTAINS Destination Network Domain [or]
Destination Network Domain CONTAINS Source HostName
AND
Account Name NOT EQUAL TO - [and]
Account Name DOES NOT CONTAIN $ [and]
Account Name DOES NOT CONTAIN ANONYMOUS [and]
Account Name DOES NOT CONTAIN LOCAL [and]
Destination Network Domain DOES NOT CONTAIN PROD

Risk Boosters
Active List:
accountname in suspicious_host_accessed [and/or]
employeeid in:

Possible_bruteforce
- suspicious_host_accessed
- suspicious_process_anomaly
- suspicious_AD_authentication
- possible_privilege_misuse
- vulnerable_endpoints
- infected_endpoints

increase factor 4.0

Verbose Info
Account: ${accountname!"ACCOUNTNAME"} IP address: ${ipaddress!"UNKNOWN"} Host: ${resourcename!"UNKNOWN"} Destination User: ${destinationusername!"UNKNOWN"} Account Domain:

${destinationntdomain!"UNKNOWN"} Message: ${message!"UNKNOWN"} EventID: ${baseeventid!"UNKNOWN"}

Response Bot Fields/Attributes/Policies

Account Created and Deleted-13
Account Created and Deleted
Abnormal number of account creation
Rare local account created
Abnormal number of account creation-disabled
Rare host accessed by an account - Logon Failure
Local accounts created on windows

Member Added to Built-In Admin Groups by Uncorrelated Accounts

Criticality: Low
Applies to: Functionality
Policy Category: Account Misuse

Device Category

Windows

Description

Adding members to built-in admin group could indicate a possible privilege escalation.

Analytical Type

Real Time Policy

Prerequisites

- windows logs
- HR Data
- User Data

Violation Entity

Resource Group Account

Threat Focus Area

Cyber

Threat Indicator

Member added to built-in admin groups by uncorrelated accounts

Kill Chain Stage

Recon

Remediation Steps

- Nessus LaunchScan
- NessusConnector StopScan
- NessusConnector FetchScan
- AD BlockUser
- AD UnBlockUser
- Tanium - Machine Information
- Tanium - Running Processes with MD5

- Tanium - Running Applciations
- Tanium - Non-approved Established Connections

Detection Algorithm
Individual Event Analytics

Criteria to Filter Event
baseeventid EQUAL TO 4732 [or]
baseeventid EQUAL TO 636
AND
devicecustomstring1 EQUAL TO Administrators [or]
devicecustomstring1 EQUAL TO Power Users
AND
user id equal to -1

Verbose Info
Account: ${accountname!"ACCOUNTNAME"} IP address: ${ipaddress!"UNKNOWN"} Host: ${resourcename!"UNKNOWN"} Group Name: ${devicecustomstring1$LIST!"UNKNOWN"} Destination User: ${destinationusername!"UNKNOWN"} Message: ${message!"UNKNOWN"} EventID: ${baseeventid!"UNKNOWN"}

Response Bot Fields/Attributes/Policies
A member was added and removed from a security enabled group within a short time-13
Account added and removed to security group
Rare builtin member group additions
Restricted Group Change
A member was added and removed from a security enabled group within a short time-17

New Admin Account Detected
Criticality: None
Applies to: Functionality
Policy Category: Account Misuse

Device Category
Windows

Description
Undocumented admin authentication could indicate a malicious activity.

Technique Used
Behavior anomaly on accounts with admin privileges

Analytical Type
Tier 2 Behavior Summary

Prerequisites
- windows logs
- Behavior profiles

Violation Entity
Resource Group Account

Threat Focus Area
Insider/Cyber

Threat Indicator
Possible unauthorized access

Kill Chain Stage
Recon

Remediation Steps
- AD BlockUser
- AD UnBlockUser

Detection Algorithm
Rare Behavior

Criteria to Filter Event
baseid equal to 4672
AND
Account Name NOT EQUAL TO - [and]
Account Name DOES NOT CONTAIN $ [and]
Account Name DOES NOT CONTAIN LOCAL [and]
Account Name DOES NOT CONTAIN ANONYMOUS

Risk Boosters
Match Critera:
Destination user privileges contains SeDebugPrivilege [or]
Destination user privileges contains SeImpersonatePrivilege [or]
Destination user privileges contains SeAuditPrivilege
increase factor 2.0

Verbose Info
Account: ${accountname!"ACCOUNTNAME"} IP address: ${ipaddress!"UNKNOWN"} Host: ${resourcename!"UNKNOWN"} Destination User: ${destinationusername!"UNKNOWN"} Message: ${message!"UNKNOWN"} EventID: ${baseeventid!"UNKNOWN"}

Response Bot Fields/Attributes/Policies
Possible Privilege Escalation - Self Escalation
Rare local account created

Pass the Hash Detection–Key Length Analysis
Criticality: None
Applies to: Functionality
Policy Category: Account Misuse

Device Category
Windows

Description
This is an indicator of lateral movement being observed via the pass the hash technique.

Analytical Type
Real Time Policy

Prerequisites
- windows logs
- IP atributions

Violation Entity
Resource Group Account

Threat Focus Area
Cyber

Threat Indicator
Suspicious AD Authentication

Kill Chain Stage
Recon

Remediation Steps
- AD BlockUser
- AD UnBlockUser
- Tanium - Machine Information
- Tanium - Running Processes with MD5
- Tanium - Running Applciations
- Tanium - Non-approved Established Connections

Detection Algorithm
Individual event analytics

Criteria to Filter Event
baseeventid EQUAL TO 4624 [or]
baseeventid EQUAL TO 4625
AND
CustomNumber 1 EQUAL TO 3.0 [and]
requestclientapplication CONTAINS NTLM [and]
CustomNumber 3 EQUAL TO 0

Verbose Info
Account ${accountname!"ACCOUNTNAME"} performed ${transactionstring1!"ACTIVITY"} from ipaddress ${ipaddress!"UNKNOWN"}

Response Bot Fields/Attributes/Policies
Password hash access
Suspicious Account Activity - Potential pass-the-hash - Host Length Analytic
Suspicious Account Activity - Potential pass-the-hash - Key Length Analytic
Suspicious Process Activity - Potential Mimikatz or Hash Passing Token Creation - Powershell Privileged Service Call Analytic
Suspicious Process Activity - Endpoint - Potential Mimikatz Object Handling Activity Analytic
Pass the hash detection - Randomly generated hosts

Pass the Hash Detection– Randomly Generated Hosts
Criticality: Low

Applies to: Functionality
Policy Category: Account Misuse

Device Category
Windows

Description
Detects pass the hash from randomly generated hosts.

Analytical Type
Tier 2 Behavior Summary

Prerequisites
- windows logs
- Behavior profiles

Violation Entity
Resource Group Account

Threat Focus Area
Cyber

Threat Indicator
Suspicious AD Authentication

Kill Chain Stage
Recon

Remediation Steps
- AD BlockUser
- AD UnBlockUser
- Tanium - Machine Information
- Tanium - Running Processes with MD5
- Tanium - Running Applciations
- Tanium - Non-approved Established Connections

Detection Algorithm
Rare Behavior

Criteria to Filter Event
baseeventid EQUAL TO 4624 [or]
baseeventid EQUAL TO 4776 [or]
baseeventid EQUAL TO 4625
AND
customnumber 3 equal to 16.0

Verbose Info

Account ${accountname!"ACCOUNTNAME"} performed ${transactionstring1!"ACTIVITY"} from ipaddress ${ipaddress!"UNKNOWN"}

Response Bot Fields/Attributes/Policies

Password hash access
Suspicious Account Activity - Potential pass-the-hash - Host Length Analytic
Suspicious Account Activity - Potential pass-the-hash - Key Length Analytic
Suspicious Process Activity - Potential Mimikatz or Hash Passing Token Creation - Powershell Privileged Service Call Analytic
Pass the hash detection - Key length analysis
Suspicious Account Activity - Peak Credential Validation Failure Increase For Host Analytic
Suspicious Process Activity - Endpoint - Potential Mimikatz Object Handling Activity Analytic

---

Password Reset Anomaly

Criticality: None
Applies to: Functionality
Policy Category: Account Misuse

Device Category

Windows

Description

This may be indicative of a possible account takeover attempt as these are not self-password reset events

Technique Used

Entity attribution

Analytical Type

Real Time Policy

Prerequisites

- windows logs

Violation Entity

Resource Group Account

Threat Focus Area

Insider/Cyber

Threat Indicator

Possible privilege misuse

Kill Chain Stage

Delivery

Remediation Steps

- AD BlockUser
- AD UnBlockUser
- Tanium - Machine Information
- Tanium - Running Processes with MD5
- Tanium - Running Applciations

- Tanium - Non-approved Established Connections

Detection Algorithm
Individual event analytics

Criteria to Filter Event
baseeventid EQUAL TO 4723 [and]
u_id NOT EQUAL TO -1
AND
Account Name NOT EQUAL TO Destination User Name [and]
Account Name DOES NOT CONTAIN $ [and]
Account Name NOT EQUAL TO - [and]
Account Name DOES NOT CONTAIN ANONYMOUS [and]
Account Name DOES NOT CONTAIN LOCAL

Risk Boosters
Active List:
accountname in suspicious_host_accessed [and/or]
employeeid in:
- Possible_bruteforce
- suspicious_process_anomaly
- suspicious_AD_authentication
- possible_privilege_misuse
- vulnerable_endpoints
- infected_endpoints
increase factor 4.0

Verbose Info
Account: ${accountname!"ACCOUNTNAME"} IP address: ${ipaddress!"UNKNOWN"} Host: ${resourcename!"UNKNOWN"} Destination User: ${destinationusername!"UNKNOWN"} Message: ${message!"UNKNOWN"} EventID: ${baseeventid!"UNKNOWN"}

Response Bot Fields/Attributes/Policies
Abnormal number of domain password reset attempts-SIEM-13
Abnormal number of domain password reset attempts
Abnormal number of domain password reset attempts-SIEM-17

Possible Password Spraying from a Resource
Criticality: Low
Applies to: Functionality
Policy Category: Account Misuse

Device Category
Windows

Description
A bruteforce attempt from a source host, whereby the same password wis tried against a list of user accounts.

Analytical Type
Tier 2 Behavior Summary

Prerequisites
- windows logs
- Behavior profiles

Violation Entity
Resources

Threat Focus Area
Insider/Cyber

Threat Indicator
Suspicious AD Authentication

Kill Chain Stage
Recon

Remediation Steps
- AD BlockUser
- AD UnBlockUser
- Tanium - Machine Information
- Tanium - Running Processes with MD5
- Tanium - Running Applciations
- Tanium - Non-approved Established Connections

Detection Algorithm
Enumeration behavior

Criteria to Filter Event
baseeventid equal to 624 [or]

baseeventid EQUAL TO 4625 [or]
baseeventid EQUAL TO 529
AND
Account Name NOT EQUAL TO - [and]
Account Name DOES NOT CONTAIN ANONYMOUS [and]
Account Name DOES NOT CONTAIN LOCAL [and]
Account Name DOES NOT CONTAIN $

Verbose Info
IP address: ${ipaddress!"UNKNOWN"} Host: ${resourcename!"UNKNOWN"} Message: ${message!"UNKNOWN"} EventID: ${baseeventid!"UNKNOWN"}

Response Bot Fields/Attributes/Policies
Possible password spraying from an ipaddress
High number of accounts used on a workstation for successful authentications or run as events
High number of accounts from the same ipaddress for successful authentications or run as events
High number of accounts from the same ipaddress for authentication failures or lockout events

Possible Password Spraying from an IP Address
Criticality: Low
Applies to: Functionality
Policy Category: Account Misuse

Device Category
Windows

Description
Possible brute force attempt to logon to an account

Analytical Type
Tier 2 Behavior Summary

Prerequisites
- windows logs
- Behavior profiles

Violation Entity
Network Address

Threat Focus Area
Insider/Cyber

Threat Indicator
Suspicious AD Authentication

Kill Chain Stage
Recon

Remediation Steps
- AD BlockUser
- AD UnBlockUser
- Tanium - Machine Information
- Tanium - Running Processes with MD5
- Tanium - Running Applciations
- Tanium - Non-approved Established Connections

Detection Algorithm
Enumeration behavior

Criteria to Filter Event
baseeventid EQUAL TO 4625 [or]
baseeventid EQUAL TO 529
AND
Account Name NOT EQUAL TO - [and]
Account Name DOES NOT CONTAIN ANONYMOUS [and]
Account Name DOES NOT CONTAIN LOCAL [and]
Account Name DOES NOT CONTAIN $

Verbose Info
IP address: ${ipaddress!"UNKNOWN"} Host: ${resourcename$LIST!"UNKNOWN"} Message: ${message!"UNKNOWN"} EventID: ${baseeventid!"UNKNOWN"}

Response Bot Fields/Attributes/Policies
Possible password spraying from a resource
High number of accounts used on a workstation for successful authentications or run as events
High number of accounts from the same ipaddress for successful authentications or run as events
High number of accounts from the same ipaddress for authentication failures or lockout events

---

Possible Privilege Escalation–Self Escalation
Criticality: Medium
Applies to: Functionality
Policy Category: Account Misuse

Device Category
Windows

Description
This may be indicative of a privilege abuse activity by users to escalate privileges on their local accounts

Technique Used
Entity attribution

Analytical Type
Real Time Policy

Prerequisites
- windows logs

Violation Entity
Resource Group Account

Threat Focus Area
Insider/Cyber

Threat Indicator
Possible Escalation of Privileges

Kill Chain Stage
Recon

Remediation Steps
- Nessus LaunchScan
- NessusConnector StopScan
- NessusConnector FetchScan
- AD BlockUser
- AD UnBlockUser
- Tanium - Machine Information
- Tanium - Running Processes with MD5

- Tanium - Running Applciations
- Tanium - Non-approved Established Connections

Detection Algorithm
Individual event analytics

Criteria to Filter Event
u_id NOT EQUAL TO -1
AND
baseeventid EQUAL TO 4720 [or]
baseeventid EQUAL TO 4728 [or]
baseeventid EQUAL TO 4732 [or]
baseeventid EQUAL TO 4756
AND
User ID CONTAINS Destination User Id [or]
Destination User Id CONTAINS User ID [or]
Account Name CONTAINS Destination User Name [or]
Destination User Name CONTAINS Account Name
AND
Account Name NOT EQUAL TO - [and]
Account Name DOES NOT CONTAIN ANONYMOUS [and]
Account Name DOES NOT CONTAIN LOCAL [and]
Account Name DOES NOT CONTAIN $

Verbose Info
Account: ${accountname!"ACCOUNTNAME"} IP address: ${ipaddress!"UNKNOWN"} Host: ${resourcename!"UNKNOWN"} Destination User: ${destinationuserid!"UNKNOWN"} Message: ${message!"UNKNOWN"} EventID: ${baseeventid!"UNKNOWN"}

Response Bot Fields/Attributes/Policies
Rare privileged events performed by user compared to peer
Rare privileged level for windows authentication

Possible Remote Interactive Logon Enumeration
Criticality: Low
Applies to: Functionality
Policy Category: Account Misuse

Device Category
Windows

Description
Enumeration behavior observed on interactive logon

Analytical Type
Tier 2 Behavior Summary

Prerequisites
- windows logs
- Behavior profiles

Violation Entity
Resource Group Account

Threat Focus Area
Insider/Cyber

Threat Indicator
Suspicious AD Authentication

Kill Chain Stage
Recon

Remediation Steps
- AD BlockUser
- AD UnBlockUser
- Tanium - Machine Information
- Tanium - Running Processes with MD5
- Tanium - Running Applciations
- Tanium - Non-approved Established Connections

Detection Algorithm
Enumeration behavior

Criteria to Filter Event
baseeventid EQUAL TO 4624 [or]
baseeventid EQUAL TO 528
AND
Account Name DOES NOT CONTAIN LOCAL [and]
CustomNumber 1 EQUAL TO 10.0 [and]
Account Name DOES NOT CONTAIN $ [and]
Account Name NOT EQUAL TO - [and]
Account Name DOES NOT CONTAIN ANONYMOUS [and]
Account Name DOES NOT CONTAIN SYSTEM [and]
Account Name DOES NOT CONTAIN Window Manager [and]
Account Name DOES NOT CONTAIN DWM

Verbose Info
IP address: ${ipaddress!"UNKNOWN"} Host: ${resourcename!"UNKNOWN"} Message: ${message!"UNKNOWN"} EventID: ${baseeventid!"UNKNOWN"}

Response Bot Fields/Attributes/Policies
Abnormal number of remote interactive logon from an account-SIEM-13
Use of explicit credentials - Account sharing or Password misuse
Abnormal number of accounts enumerated
Rare account enumeration event
Rare target account authentication using explicit credentials
Suspicious Account Activity - Potential pass-the-hash - Host Length Analytic
Suspicious Account Activity - Potential pass-the-hash - Key Length Analytic
Suspicious Account Activity - Peak Credential Validation Failure Increase For Host Analytic
Suspicious Account Activity - Kerberoasting - Peak TGS Request For User Analytic
Suspicious Account Activity - Peak Explicit Credentials Distinct Account Name For Host Analytic

Rare Account Enumeration Event
Criticality: Low
Applies to: Functionality

Policy Category: Account Misuse

Device Category
Windows

Description
This policy detects the occurrence of an account enumeration event for the first time

Analytical Type
Tier 2 Behavior Summary

Prerequisites
- windows logs
- Behavior profiles

Violation Entity
Resource Group Account

Threat Focus Area
Cyber

Threat Indicator
Possible account enumeration

Kill Chain Stage
Exploit

Remediation Steps
- Nessus LaunchScan
- NessusConnector StopScan
- NessusConnector FetchScan
- AD BlockUser
- AD UnBlockUser
- Tanium - Machine Information
- Tanium - Running Processes with MD5
- Tanium - Running Applciations
- Tanium - Non-approved Established Connections

Detection Algorithm
Rare behavior

Criteria to Filter Event
baseeventid EQUAL TO 4798 [and]
Account Name DOES NOT CONTAIN $ [and]
Account Name DOES NOT CONTAIN LOCAL [and]
Account Name DOES NOT CONTAIN ANONYMOUS [and]
Account Name NOT EQUAL TO -

Verbose Info
Account: ${accountname!"ACCOUNTNAME"} IP address: ${ipaddress!"UNKNOWN"} Host: ${resourcename!"UNKNOWN"} Message: ${message!"UNKNOWN"} EventID: ${baseeventid!"UNKNOWN"}

Response Bot Fields/Attributes/Policies
Possible AD Enumeration
Abnormal number of privileges enumerated
Abnormal number of accounts enumerated
Rare privilege enumeration event
Abnormal number of account enumeration attempts on an endpoint
Possible Privilege Enumeration
Suspicious AD Enumeration Observed

Rare Admin Group Member Additions by User Compared to Peer
Criticality: Low
Applies to: Functionality
Policy Category: Account Misuse

Device Category
Windows

Description
Rare admin group member additions compared to peers could be indicative of privilege misuse activity

Technique Used
Behavior anomaly on admin group member additions by peer

Analytical Type
Tier 2 Behavior Summary

Prerequisites
- windows logs
- Behavior profiles

Violation Entity
Resource Group Account

Threat Focus Area
Insider/Cyber

Threat Indicator
Possible privilege misuse

Kill Chain Stage
Delivery

Remediation Steps
- AD BlockUser
- AD UnBlockUser
- Tanium - Machine Information
- Tanium - Running Processes with MD5
- Tanium - Running Applications
- Tanium - Non-approved Established Connections

Detection Algorithm
Abnormal activity compared to peers

Criteria to Filter Event

baseeventid EQUAL TO 4732 [or]
baseeventid EQUAL TO 636
AND
devicecustomstring1 EQUAL TO Power Users [and]
devicecustomstring1 EQUAL TO Administrators
AND
Account Name NOT EQUAL TO - [and]
Account Name DOES NOT CONTAIN LOCAL [and]
Account Name DOES NOT CONTAIN ANONYMOUS [and]
Account Name DOES NOT CONTAIN $

Risk Boosters

active list:
accountname in:
- suspicious_host_accessed
- possible_bruteforce
- suspicious_process_anomaly
- suspicious_ad_authentication
- possible privilege_misuse
- vulnerable_endpoints
- infected_endpoints

Verbose Info

Account: ${accountname!"ACCOUNTNAME"} IP address: ${ipaddress!"UNKNOWN"} Host: ${resourcename!"UNKNOWN"} Destination User: ${destinationusername!"UNKNOWN"} Message: ${message!"UNKNOWN"} EventID: ${baseeventid!"UNKNOWN"}

Response Bot Fields/Attributes/Policies

Abnormal number of domain password reset attempts-SIEM-13
Detection of Domain Trust Additions - Peer anomaly
Firewall disabled on windows
Rare audit log clearing by an account
Rare registry modification by an account
Rare regedit usage compared to peer
Password hash access
Rare process creation on an endpoint
Rare privileged events performed by user compared to peer
Suspicious Service creation
Rare service created on endpoint
Rare token elevation for process
Rare password reset for domain admin
Rare local account created
Audit Log Tampering
Member added to built-in admin groups by uncorelated accounts
Use of credential dumpers
Abnormal number of domain password reset attempts
Firewall configurations modified on windows
Rare builtin member group additions
Audit policy changes
Restricted Group Change
Possible local account created
Domain account creation by users
Suspicious AD policy change
Suspicious executables on a machine
Scheduled Task Creation
Local accounts created on windows

A member was added and removed from a security enabled group within a short time-17
Abnormal number of domain password reset attempts-SIEM-17

Rare Admin Share Access by an Account

Criticality: None
Applies to: Functionality
Policy Category: Account Misuse

Device Category

Windows

Description

This may be indicative of an account accessing new network objects could indicate a possible snooping or a recon activity

Technique Used

Behavior anomaly on the object access activity

Analytical Type

Tier 2 Behavior Summary

Prerequisites

- windows logs
- Behavior profiles

Violation Entity

Resource Group Account

Threat Focus Area

Cyber

Threat Indicator

Suspicious Network Share Access

Kill Chain Stage

Recon

Remediation Steps

- Nessus LaunchScan
- NessusConnector StopScan
- NessusConnector FetchScan
- AD BlockUser
- AD UnBlockUser
- Tanium - Machine Information
- Tanium - Running Processes with MD5
- Tanium - Running Applciations
- Tanium - Non-approved Established Connections

Detection Algorithm

Rare behavior

Criteria to Filter Event

baseeventid EQUAL TO 4663
AND
Account Name DOES NOT CONTAIN $ [and]
Account Name DOES NOT CONTAIN ANONYMOUS [and]
Account Name DOES NOT CONTAIN LOCAL [and]
Account Name NOT EQUAL TO -

Verbose Info

Account: ${accountname!"ACCOUNTNAME"} Object Type: ${devicecustomstring1!"UNKNOWN"} Host: ${resourcename!"UNKNOWN"} Object Name: ${devicecustomstring2!"UNKNOWN"} Message: ${message!"UNKNOWN"} EventID: ${baseeventid!"UNKNOWN"}

Response Bot Fields/Attributes/Policies

Abnormal number of administrative share object accessed-SIEM-13
Abnormal object or network share access attempts-SIEM-13
Abnormal number of network share object access
Abnormal number of administrative share object accessed
Spike in administrative shares accessed
Unusual high number of network shares accessed - SIEM
Abnormal number of administrative share object accessed-SIEM-17
Abnormal number of hosts accessed-SIEM-17
Suspicious host access behavior from an account
Rare Host Accessed from an Account
Rare Host Accessed Attempt By Account
Rare host accessed by an account - Logon Failure
Rare host accessed by an account - Logon Success
Abnormal number of hosts accessed
Abnormal number of host access attempts
Rare host accessed by an account
Abnormal number of hosts accessed-SIEM-13

Rare Audit Log Clearing by an Account

Criticality: Low
Applies to: Functionality
Policy Category: Account Misuse

Device Category

Windows

Description

This may be indicative of an audit log tampering activity

Technique Used

Behavior anomaly on audit log clearing activity

Analytical Type

Tier 2 Behavior Summary

Prerequisites

- windows logs
- Behavior profiles

Violation Entity
Resource Group Account

Threat Focus Area
Insider/Cyber

Threat Indicator
Audit log tampering

Kill Chain Stage
Exploit

Remediation Steps
- Nessus LaunchScan
- NessusConnector StopScan
- NessusConnector FetchScan
- AD BlockUser
- AD UnBlockUser
- Tanium - Machine Information
- Tanium - Running Processes with MD5
- Tanium - Running Applciations
- Tanium - Non-approved Established Connections

Detection Algorithm
Rare behavior

Criteria to Filter Event
baseeventid EQUAL TO 1102 [or]
baseeventid EQUAL TO 517
AND
Account Name DOES NOT CONTAIN ANONYMOUS [and]
Account Name DOES NOT CONTAIN $ [and]
Account Name DOES NOT CONTAIN LOCAL [and]
Account Name NOT EQUAL TO -

Risk Boosters
Active List:
accountname in suspicious_host_accessed [and/or]
employeeid in:
- Possible_bruteforce
- suspicious_process_anomaly
- suspicious_AD_authentication
- possible_privilege_misuse
- vulnerable_endpoints
- infected_endpoints

increase factor 4.0

Verbose Info
Account: ${accountname!"ACCOUNTNAME"} IP address: ${ipaddress!"UNKNOWN"} Host: ${resourcename!"UNKNOWN"} Message: ${messaage!"UNKNOWN"} EventID: ${baseeventid!"UNKNOWN"}

Response Bot Fields/Attributes/Policies

Audit Log Tampering
Audit policy changes
Detection of Domain Trust Additions - Peer anomaly
Member added to built-in admin groups by uncorelated accounts
Rare builtin member group additions
Rare admin group member additions by user compared to peer
Firewall disabled on windows
Firewall configurations modified on windows
Scheduled Task Creation
Local accounts created on windows
Possible local account created
Rare local account created
Rare service created on endpoint
Local accounts created on windows - Target domain analysis
Rare regedit usage compared to peer
Rare registry modification by an account
Rare process creation on an endpoint
Password hash access
Rare Basic Service Operation
Rare password reset for domain admin
Restricted Group Change
Domain account creation by users
Suspicious Registry Modification Observed

Rare Authentication Domain Detected

Criticality: Low
Applies to: Functionality
Policy Category: Account Misuse

Device Category

Windows

Description

Detects authentication from a rare domain that can indicate account misuse or an attacker sneaking in through a trusted domain that has been added.

Analytical Type

Tier 2 Behavior Summary

Prerequisites

- windows logs
- Behavior profiles

Violation Entity

Resource Group Account

Threat Focus Area

Insider/Cyber

Threat Indicator

Suspicious AD Authentication

Kill Chain Stage

Recon

Remediation Steps
- AD BlockUser
- AD UnBlockUser
- Tanium - Machine Information
- Tanium - Running Processes with MD5
- Tanium - Running Applciations
- Tanium - Non-approved Established Connections

Detection Algorithm
Rare behavior

Criteria to Filter Event
baseeventid EQUAL TO 4624 [or]
baseeventid EQUAL TO 4625 [or]
baseeventid EQUAL TO 4776
AND
Destination Network Domain IS NOT NULL

Verbose Info
Account ${accountname!"ACCOUNTNAME"} performed ${transactionstring1!"ACTIVITY"} from ipaddress ${ipaddress!"UNKNOWN"}

Response Bot Fields/Attributes/Policies
Detection of Domain Trust Additions - Peer anomaly
- not sure what else to add here as suspicious authentication could be almost on logon events and it should be related

---

Rare Built-in Member Group Additions
Criticality: Low
Applies to: Functionality
Policy Category: Account Misuse

Device Category
Windows

Description
Detects rare built-in member group additions that could indicate an attacker elevating an account with addition rights, if a local machine account they are attempting to circumvent controls by hiding activities from the domain due to only being logged in the workstation logs.

Analytical Type
Tier 2 Behavior Summary

Prerequisites
- windows logs
- Behavior profiles

Violation Entity
Resource Group Account

Threat Focus Area
Insider/Cyber

Threat Indicator
Possible privilege misuse

Kill Chain Stage
Delivery

Remediation Steps
- AD BlockUser
- AD UnBlockUser
- Tanium - Machine Information
- Tanium - Running Processes with MD5
- Tanium - Running Applciations
- Tanium - Non-approved Established Connections

Detection Algorithm
Rare behavior

Criteria to Filter Event
baseeventid EQUAL TO 4732 [or]
baseeventid EQUAL TO 636 [or]
baseeventid EQUAL TO 4728 [or]
baseeventid EQUAL TO 4756 [or]
devicecustomstring1 EQUAL TO Power Users [or]
devicecustomstring1 EQUAL TO Administrators
AND
Account Name NOT EQUAL TO - [and]
Account Name DOES NOT CONTAIN LOCAL [and]
Account Name DOES NOT CONTAIN ANONYMOUS [and]
Account Name DOES NOT CONTAIN $

Risk Boosters
active list:
accountname in:
- suspicious_host_accessed
- possible_bruteforce
- suspicious_process_anomaly
- suspicious_ad_authentication
- possible privilege_misuse
- vulnerable_endpoints
- infected_endpoints

Verbose Info

Account: ${accountname!"ACCOUNTNAME"} IP address: ${ipaddress!"UNKNOWN"} Host: ${resourcename!"UNKNOWN"} Destination User: ${destinationusername!"UNKNOWN"} Message: ${message!"UNKNOWN"} EventID: ${baseeventid!"UNKNOWN"}

Response Bot Fields/Attributes/Policies

A member was added and removed from a security enabled group within a short time-13
Account added and removed to security group
Member added to built-in admin groups by uncorelated accounts
Rare admin group member additions by user compared to peer
A member was added and removed from a security enabled group within a short time-17

Rare Host Accessed Attempt by Account

Criticality: Low
Applies to: Functionality
Policy Category: Account Misuse

Device Category

Windows

Description

A rare login attempt activity by account indicate a possible account takeover or a lateral propagation attempt

Technique Used

Behavior anomaly on the hosts typically accessed by an account

Analytical Type

Tier 2 Behavior Summary

Prerequisites

- windows logs
- Behavior profiles

Violation Entity

Resource Group Account

Threat Focus Area

Insider/Cyber

Threat Indicator

Suspicious AD Authentication

Kill Chain Stage

Recon

Remediation Steps

- AD BlockUser
- AD UnBlockUser
- Tanium - Machine Information
- Tanium - Running Processes with MD5
- Tanium - Running Applciations
- Tanium - Non-approved Established Connections

Detection Algorithm
Rare behavior

Criteria to Filter Event
Account Name IS NOT NULL [and]
Account Name NOT EQUAL TO - [and]
Account Name DOES NOT CONTAIN $ [and]
Source HostName DOES NOT CONTAIN ADS [and]
Source HostName DOES NOT CONTAIN ADC [and]
Account Name DOES NOT CONTAIN ANONYMOUS [and]
Account Name DOES NOT CONTAIN LOCAL
AND
baseeventid EQUAL TO 4625 [or]
baseeventid EQUAL TO 4624 [or]
baseeventid EQUAL TO 4776

Verbose Info
Account ${accountname!"ACCOUNTNAME"} performed ${transactionstring1!"ACTIVITY"} from ipaddress ${ipaddress!"UNKNOWN"}

Response Bot Fields/Attributes/Policies
Abnormal number of hosts accessed-SIEM-13
Rare host accessed by an account
Abnormal number of host access attempts
Abnormal number of hosts accessed
Rare host accessed by an account - Logon Success
Rare host accessed by an account - Logon Failure
Rare Host Accessed from an Account
Suspicious host access behavior from an account
Abnormal number of hosts accessed-SIEM-17
Abnormal number of administrative share object accessed-SIEM-17
Rare object access attempts by an account
Abnormal number of administrative share object accessed
Abnormal number of network share object access
Rare admin share access by an account
Abnormal object or network share access attempts-SIEM-13
Abnormal number of administrative share object accessed-SIEM-13
Abnormal object or network share access attempts by resource-SIEM-13

Rare Host Accessed by an Account
Criticality: None
Applies to: Functionality
Policy Category: Account Misuse

Device Category
Windows

Description
A spike in account accessing new hosts could indicate a possible account takeover or a lateral propagation attempt

Technique Used
Behavior anomaly on the hosts typically accessed by an account

Analytical Type
Tier 2 Behavior Summary

Prerequisites
- windows logs
- Behavior profiles

Violation Entity
Suspicious AD Authentication

Threat Focus Area
Insider/Cyber

Threat Indicator
Possible privilege misuse

Kill Chain Stage
Recon

Remediation Steps
- AD BlockUser
- AD UnBlockUser
- Tanium - Machine Information
- Tanium - Running Processes with MD5
- Tanium - Running Applciations
- Tanium - Non-approved Established Connections

Detection Algorithm
Rare behavior

Criteria to Filter Event
baseeventid EQUAL TO 4624 [oe]
baseeventid EQUAL TO 528 [or]
baseeventid EQUAL TO 540 [or]
baseeventid EQUAL TO 4776
AND
Account Name IS NOT NULL [and]
Account Name DOES NOT CONTAIN $ [and]
Account Name NOT EQUAL TO - [and]
Account Name DOES NOT CONTAIN LOCAL [and]
Account Name DOES NOT CONTAIN ANONYMOUS

Verbose Info
Account: ${accountname!"ACCOUNTNAME"} IP address: ${ipaddress!"UNKNOWN"} Host: ${resourcename!"UNKNOWN"} Message: ${message!"UNKNOWN"} EventID: ${baseeventid!"UNKNOWN"}

Response Bot Fields/Attributes/Policies
Abnormal object or network share access attempts by resource-SIEM-13
Abnormal number of administrative share object accessed-SIEM-13
Abnormal object or network share access attempts-SIEM-13
Rare admin share access by an account
Abnormal number of network share object access

Abnormal number of administrative share object accessed
Spike in administrative shares accessed
Unusual high number of network shares accessed - SIEM
Abnormal number of administrative share object accessed-SIEM-17
Abnormal number of hosts accessed-SIEM-17
Suspicious host access behavior from an account
Rare Host Accessed from an Account
Rare Host Accessed Attempt By Account
Rare host accessed by an account - Logon Failure
Rare host accessed by an account - Logon Success
Abnormal number of hosts accessed
Abnormal number of host access attempts
Abnormal number of hosts accessed-SIEM-13

Rare Host Accessed by an Account–Logon Failure

Criticality: None
Applies to: Functionality
Policy Category: Account Misuse

Device Category

Windows

Description

A spike in account accessing new hosts could indicate a possible account takeover or a lateral propagation attempt

Technique Used

Behavior anomaly on the hosts typically accessed by an account

Analytical Type

Tier 2 Behavior Summary

Prerequisites

- windows logs
- Behavior profiles
- Naming Convention for Domain admin Accounts

Violation Entity

Resource Group Account

Threat Focus Area

Insider/Cyber

Threat Indicator

Suspicious AD Authentication

Kill Chain Stage

Recon

Remediation Steps

- AD BlockUser
- AD UnBlockUser
- Tanium - Machine Information
- Tanium - Running Processes with MD5

- Tanium - Running Applciations
- Tanium - Non-approved Established Connections

Detection Algorithm

Rare Behavior

Criteria to Filter Event

baseeventid EQUAL TO 4625 [or]
baseeventid EQUAL TO 529 [or]
baseeventid EQUAL TO 530 [or]
baseeventid EQUAL TO 532 [or]
baseeventid EQUAL TO 531 [or]
baseeventid EQUAL TO 533 [or]
baseeventid EQUAL TO 534 [or]
baseeventid EQUAL TO 535 [or]
baseeventid EQUAL TO 536 [or]
baseeventid EQUAL TO 537 [or]
baseeventid EQUAL TO 538 [or]
baseeventid EQUAL TO 539 [or]
baseeventid EQUAL TO 4776
AND
Destination HostName DOES NOT START WITH ADS [and]
Destination HostName DOES NOT START WITH ADC
AND
Account Name DOES NOT CONTAIN $ [and]
Account Name DOES NOT CONTAIN LOCAL [and]
Account Name DOES NOT CONTAIN ANONYMOUS [and]
Account Name NOT EQUAL TO -

Verbose Info

Account: ${accountname!"ACCOUNTNAME"} IP address: ${ipaddress!"UNKNOWN"} Host: ${resourcename!"UNKNOWN"} Message: ${message!"UNKNOWN"} EventID: ${baseeventid!"UNKNOWN"}

Response Bot Fields/Attributes/Policies

Abnormal number of hosts accessed-SIEM-13
Rare host accessed by an account
Abnormal number of host access attempts
Abnormal number of hosts accessed
Rare host accessed by an account - Logon Success
Rare Host Accessed Attempt By Account
Rare Host Accessed from an Account
Suspicious host access behavior from an account
Abnormal number of hosts accessed-SIEM-17
Abnormal number of administrative share object accessed-SIEM-17
Unusual high number of network shares accessed - SIEM
Spike in administrative shares accessed
Abnormal number of administrative share object accessed
Abnormal number of network share object access
Rare admin share access by an account
Abnormal object or network share access attempts-SIEM-13
Abnormal number of administrative share object accessed-SIEM-13
Abnormal object or network share access attempts by resource-SIEM-13

Rare Host Accessed from an Account

Criticality: Low

Applies to: Functionality
Policy Category: Account Misuse

Device Category
Windows

Description
Detects that the account has accessed a system they would not normally, which can be an indicator of insider taking advantage of those privileges or more malicious activity.

Analytical Type
Tier 2 Behavior Summary

Prerequisites
- windows logs
- Behavior profiles

Violation Entity
Resource Group Account

Threat Focus Area
Cyber

Threat Indicator
Lateral Movement

Kill Chain Stage
Execute

Remediation Steps
- AD BlockUser
- AD UnBlockUser
- Tanium - Machine Information
- Tanium - Running Processes with MD5
- Tanium - Running Applciations
- Tanium - Non-approved Established Connections

Detection Algorithm
Rare behavior

Criteria to Filter Event
baseeventid EQUAL TO 4624 [or]
baseeventid EQUAL TO 4625 [or]
baseeventid EQUAL TO 4776
AND
Destination HostName DOES NOT CONTAIN DC

Verbose Info

Account ${accountname!"ACCOUNTNAME"} performed ${transactionstring1!"ACTIVITY"} from ipaddress ${ipaddress!"UNKNOWN"}

Response Bot Fields/Attributes/Policies

Abnormal number of hosts accessed-SIEM-13
Rare host accessed by an account
Abnormal number of host access attempts
Abnormal number of hosts accessed
Rare host accessed by an account - Logon Success
Rare host accessed by an account - Logon Failure
Rare Host Accessed Attempt By Account
Suspicious host access behavior from an account
Abnormal number of administrative share object accessed-SIEM-13
Abnormal object or network share access attempts-SIEM-13
Rare admin share access by an account
Abnormal number of network share object access
Abnormal number of administrative share object accessed
Spike in administrative shares accessed
Unusual high number of network shares accessed - SIEM
Abnormal number of administrative share object accessed-SIEM-17

Rare Interactive Logon by Service Account

Criticality: Low
Applies to: Functionality
Policy Category: Account Misuse

Device Category

Windows

Description

Rare interactive logon for a service account indicates a change in the typical authentication pattern for a service account. This could indicate an account being misused or using unauthorized elevated privileges.

Technique Used

Behavior anomaly for rarity on logon type

Analytical Type

Tier 2 Behavior Summary

Prerequisites

- windows logs
- Behavior profiles

Violation Entity

Resource Group Account

Threat Focus Area

Insider/Cyber

Threat Indicator

Suspicious AD Authentication

Kill Chain Stage
Recon

Remediation Steps
- AD BlockUser
- AD UnBlockUser
- Tanium - Machine Information
- Tanium - Running Processes with MD5
- Tanium - Running Applciations
- Tanium - Non-approved Established Connections

Detection Algorithm
Rare behavior

Criteria to Filter Event
baseeventid EQUAL TO 4624 [or]
baseeventid EQUAL TO 528 [or]
baseeventid EQUAL TO 540
AND
CustomNumber 1 EQUAL TO 2.0 [or]
CustomNumber 1 EQUAL TO 10.0 [or]
CustomNumber 1 EQUAL TO 11.0
AND
Account Name NOT EQUAL TO - [and]
Account Name DOES NOT CONTAIN LOCAL [and]
Account Name DOES NOT CONTAIN ANONYMOUS [and]
Account Name DOES NOT CONTAIN $
AND
Account Name CONTAINS SVC [or]
Account Name CONTAINS SRV

Verbose Info
Account: ${accountname!"ACCOUNTNAME"} IP address: ${ipaddress!"UNKNOWN"} Host: ${resourcename!"UNKNOWN"} Message: ${message!"UNKNOWN"} EventID: ${baseeventid!"UNKNOWN"}

Response Bot Fields/Attributes/Policies
Service account performing interactive logon

Rare Local Account Created
Criticality: Low
Applies to: Functionality
Policy Category: Account Misuse

Device Category
Windows

Description
This policy detects the creation of a local account for the first time

Analytical Type
Tier 2 Behavior Summary

Prerequisites
- windows logs
- Behavior profiles

Violation Entity
Resource Group Account

Threat Focus Area
Cyber

Threat Indicator
Rare local account created

Kill Chain Stage
Recon

Remediation Steps
- Nessus LaunchScan
- NessusConnector StopScan
- NessusConnector FetchScan
- AD BlockUser
- AD UnBlockUser
- Tanium - Machine Information
- Tanium - Running Processes with MD5
- Tanium - Running Applciations
- Tanium - Non-approved Established Connections

Detection Algorithm
Rare behavior

Criteria to Filter Event
baseeventid EQUAL TO 4720 [OR]
baseeventid EQUAL TO 624
AND
Source HostName CONTAINS Destination Network Domain
AND
Account Name DOES NOT CONTAIN $ [and]
Account Name DOES NOT CONTAIN LOCAL [and]
Account Name DOES NOT CONTAIN ANONYMOUS [and]
Account Name NOT EQUAL TO -

Verbose Info
Account: ${accountname!"ACCOUNTNAME"} IP address: ${ipaddress!"UNKNOWN"} Host: ${resourcename!"UNKNOWN"} Destination User: ${destinationusername!"UNKNOWN"} Message: ${message!"UNKNOWN"} EventID: ${baseeventid!"UNKNOWN"}

Response Bot Fields/Attributes/Policies
Local accounts created on windows - Target domain analysis
Use of explicit credentials - Account sharing or Password misuse
Firewall disabled on windows
Rare audit log clearing by an account
Rare registry modification by an account
Detection of Domain Trust Additions - Peer anomaly
Rare regedit usage compared to peer

New admin account detected
Password hash access
Rare process creation on an endpoint
Suspicious Service creation
Rare service created on endpoint
Rare Basic Service Operation
Member added to built-in admin groups by uncorrelated accounts
Detection of possible backdoor
Firewall configurations modified on windows
Rare process detected for authentication using explicit credentials
Rare builtin member group additions
Audit policy changes
Restricted Group Change
Possible local account created
Local accounts created on windows
Scheduled Task Creation

Rare Object Access Attempts by an Account

Criticality: None
Applies to: Functionality
Policy Category: Account Misuse

Device Category

Windows

Description

This may be indicative of an account accessing new network objects could indicate a possible snooping or a recon activity

Technique Used

Behavior anomaly on the object access activity

Analytical Type

Tier 2 Behavior Summary

Prerequisites

- windows logs
- Behavior profiles

Violation Entity

Resource Group Account

Threat Focus Area

Insider/Cyber

Threat Indicator

Suspicious Network Share Access

Kill Chain Stage

Recon

Remediation Steps

- Nessus LaunchScan

- NessusConnector StopScan
- NessusConnector FetchScan
- AD BlockUser
- AD UnBlockUser
- Tanium - Machine Information
- Tanium - Running Processes with MD5
- Tanium - Running Applciations
- Tanium - Non-approved Established Connections

Detection Algorithm
Rare behavior

Criteria to Filter Event
baseeventid EQUAL TO 4663
AND
Account Name DOES NOT CONTAIN $ [and[]
Account Name DOES NOT CONTAIN ANONYMOUS [and]
Account Name DOES NOT CONTAIN LOCAL [and]
Account Name NOT EQUAL TO -

Verbose Info
Account: ${accountname!"ACCOUNTNAME"} Object Type: ${devicecustomstring1!"UNKNOWN"} Host: ${resourcename!"UNKNOWN"} Object Name: ${devicecustomstring2!"UNKNOWN"} Message: ${message!"UNKNOWN"} EventID: ${baseeventid!"UNKNOWN"}

Response Bot Fields/Attributes/Policies
Abnormal number of hosts accessed-SIEM-13
Rare host accessed by an account
Abnormal number of host access attempts
Abnormal number of hosts accessed
Rare host accessed by an account - Logon Success
Rare host accessed by an account - Logon Failure
Rare Host Accessed Attempt By Account
Rare Host Accessed from an Account
Suspicious host access behavior from an account
Abnormal number of administrative share object accessed-SIEM-17
Abnormal object or network share access attempts by resource-SIEM-13
Abnormal number of administrative share object accessed-SIEM-13
Abnormal object or network share access attempts-SIEM-13
Rare admin share access by an account
Abnormal number of network share object access
Abnormal number of administrative share object accessed
Spike in administrative shares accessed
Unusual high number of network shares accessed – SIEM

Rare Password Reset for Domain Admin
Criticality: None
Applies to: Functionality
Policy Category: Account Misuse

Device Category
Windows

Description
Rare password reset for domain admin may be indicative of a possible account takeover attempt.

Technique Used
Behavior anomaly on rare password reset for domain admins

Analytical Type
Tier 2 Behavior Summary

Prerequisites
- windows logs
- Behavior profiles

Violation Entity
Resource Group Account

Threat Focus Area
Insider/Cyber

Threat Indicator
Possible privilege misuse

Kill Chain Stage
Delivery

Remediation Steps
- AD BlockUser
- AD UnBlockUser
- Tanium - Machine Information
- Tanium - Running Processes with MD5
- Tanium - Running Applciations
- Tanium - Non-approved Established Connections

Detection Algorithm
Rare behavior

Criteria to Filter Event
baseeventid EQUAL TO 4794
AND
Account Name DOES NOT CONTAIN ANONYMOUS [and]
Account Name DOES NOT CONTAIN $ [and]
Account Name DOES NOT CONTAIN LOCAL [and]
Account Name NOT EQUAL TO -

Risk Boosters
Active List:
accountname in suspicious_host_accessed [and/or]
employeeid in:
- Possible_bruteforce
- suspicious_process_anomaly
- suspicious_AD_authentication
- possible_privilege_misuse
- vulnerable_endpoints
- infected_endpoints

increase factor 4.0

Verbose Info
Account: ${accountname!"ACCOUNTNAME"} IP address: ${ipaddress!"UNKNOWN"} Host: ${resourcename!"UNKNOWN"} Destination User: ${destinationusername!"UNKNOWN"} Message: ${message!"UNKNOWN"} EventID: ${baseeventid!"UNKNOWN"}

Response Bot Fields/Attributes/Policies
Abnormal number of domain password reset attempts-SIEM-13
Abnormal number of account creation-SIEM-13
Abnormal number of password resets-SIEM-13
Local accounts created on windows - Target domain analysis
Password Reset Anomaly
Firewall disabled on windows
Rare audit log clearing by an account
Rare registry modification by an account
Abnormal number of password resets
Abnormal number of account creation
Rare regedit usage compared to peer
New admin account detected
Rare process creation on an endpoint
Rare privileged events performed by user compared to peer
Rare Basic Service Operation
Rare local account created
Audit Log Tampering
Firewall configurations modified on windows
Rare builtin member group additions
Audit policy changes
Restricted Group Change
Possible local account created
Domain account creation by users
Scheduled Task Creation
Local accounts created on windows

Rare Privilege Enumeration Event
Criticality: Low
Applies to: Functionality
Policy Category: Account Misuse

Device Category
Windows

Description
This policy detects the occurrence of enumerating privileges for an account for the first time

Analytical Type
Tier 2 Behavior Summary

Prerequisites
- windows logs
- Behavior profiles

Violation Entity
Resource Group Account

Threat Focus Area
Insider/Cyber

Threat Indicator
Possible privilege misuse

Kill Chain Stage
Exploit

Remediation Steps
- Nessus LaunchScan
- NessusConnector StopScan
- NessusConnector FetchScan
- AD BlockUser
- AD UnBlockUser
- Tanium - Machine Information
- Tanium - Running Processes with MD5
- Tanium - Running Applciations
- Tanium - Non-approved Established Connections

Detection Algorithm
Rare behavior

Criteria to Filter Event
baseeventid EQUAL TO 4798 [or]
baseeventid EQUAL TO 4799
AND
Account Name NOT EQUAL TO - [and]
Account Name DOES NOT CONTAIN LOCAL [and]
Account Name DOES NOT CONTAIN ANONYMOUS [and]
Account Name DOES NOT CONTAIN $

Verbose Info
Account: ${accountname!"ACCOUNTNAME"} IP address: ${ipaddress!"UNKNOWN"} Host: ${resourcename!"UNKNOWN"} Message: ${message!"UNKNOWN"} EventID: ${baseeventid!"UNKNOWN"}

Response Bot Fields/Attributes/Policies
Possible AD Enumeration
Abnormal number of privileges enumerated
Abnormal number of accounts enumerated
Rare account enumeration event
Abnormal number of account enumeration attempts on an endpoint
Possible Privilege Enumeration
Suspicious AD Enumeration Observed

Rare Privileged Events Performed by User Compared to Peer
Criticality: Low
Applies to: Functionality
Policy Category: Account Misuse

Device Category
Windows

Description
This may be indicative of a privilege misuse activity

Analytical Type
Tier 2 Behavior Summary

Technique Used
Behavior anomaly on privileged event activity by peer

Prerequisites
- windows logs
- Behavior profiles

Violation Entity
Resource Group Account

Threat Focus Area
Insider/Cyber

Threat Indicator
Possible privilege misuse

Kill Chain Stage
Delivery

Remediation Steps
- AD BlockUser
- AD UnBlockUser
- Tanium - Machine Information
- Tanium - Running Processes with MD5
- Tanium - Running Applciations
- Tanium - Non-approved Established Connections

Detection Algorithm
Rare behavior

Criteria to Filter Event
baseeventid EQUAL TO 1102 [or] baseeventid EQUAL TO 4657 [or] baseeventid EQUAL TO 4706 [or]
baseeventid EQUAL TO 4720 [or] baseeventid EQUAL TO 4722 [or] baseeventid EQUAL TO 4723 [or]
baseeventid EQUAL TO 4724 [or] baseeventid EQUAL TO 4725 [or] baseeventid EQUAL TO 4726 [or]
baseeventid EQUAL TO 4727 [or] baseeventid EQUAL TO 4728 [or] baseeventid EQUAL TO 4729 [or]
baseeventid EQUAL TO 4730 [or] baseeventid EQUAL TO 4731 [or] baseeventid EQUAL TO 4732 [or]
baseeventid EQUAL TO 4733 [or] baseeventid EQUAL TO 4734 [or] baseeventid EQUAL TO 4741 [or]
baseeventid EQUAL TO 4743 [or] baseeventid EQUAL TO 4744 [or] baseeventid EQUAL TO 4746 [or]
baseeventid EQUAL TO 4747 [or] baseeventid EQUAL TO 4748 [or] baseeventid EQUAL TO 4749 [or]
baseeventid EQUAL TO 4751 [or] baseeventid EQUAL TO 4752 [or] baseeventid EQUAL TO 4753 [or]
baseeventid EQUAL TO 4754 [or] baseeventid EQUAL TO 4756 [or] baseeventid EQUAL TO 4757 [or]
baseeventid EQUAL TO 4758 [or] baseeventid EQUAL TO 4759 [or] baseeventid EQUAL TO 4761 [or]
baseeventid EQUAL TO 4762 [or] baseeventid EQUAL TO 4763 [or] baseeventid EQUAL TO 4783 [or]
baseeventid EQUAL TO 4784 [or] baseeventid EQUAL TO 4785 [or] baseeventid EQUAL TO 4786 [or]
baseeventid EQUAL TO 4787 [or] baseeventid EQUAL TO 4788 [or] baseeventid EQUAL TO 4789 [or]
baseeventid EQUAL TO 4946 [or] baseeventid EQUAL TO 4947 [or] baseeventid EQUAL TO 4950 [or]
baseeventid EQUAL TO 4954 [or] baseeventid EQUAL TO 5025 [or] baseeventid EQUAL TO 5034

AND
Account Name DOES NOT CONTAIN $ [and]
Account Name DOES NOT CONTAIN LOCAL [and]
Account Name DOES NOT CONTAIN ANONYMOUS [and]
Account Name NOT EQUAL TO -

Verbose Info
Account: ${accountname!"ACCOUNTNAME"} IP address: ${ipaddress!"UNKNOWN"} Host: ${resourcename!"UNKNOWN"} Destination User: ${destinationusername!"UNKNOWN"} Message: ${message!"UNKNOWN"} EventID: ${baseeventid!"UNKNOWN"}

Response Bot Fields/Attributes/Policies
Abnormal number of account creation-SIEM-13
Local accounts created on windows - Target domain analysis
Firewall disabled on windows
Detection of Domain Trust Additions - Peer anomaly
Rare regedit usage compared to peer
New admin account detected
Rare service created on endpoint
Rare password reset for domain admin
Rare local account created
Rare privileged level for windows authentication
Firewall configurations modified on windows
Rare builtin member group additions
Possible local account created
Domain account creation by users
Rare Host Accessed from an Account
Scheduled Task Creation
Local accounts created on windows
Rare admin group member additions by user compared to peer

Rare Regedit Usage Compared to Peer
Criticality: Medium
Applies to: Functionality
Policy Category: Account Misuse

Device Category
Windows

Description
Rare registry modification attempts may be indicative of a possible circumvention of control activity or a malicious presence on the endpoint

Analytical Type
Tier 2 Behavior Summary

Technique Used
Behavior anomaly on registry modification activity

Prerequisites
- windows logs
- Behavior profiles

Violation Entity
Resource Group Account

Threat Focus Area
Cyber

Threat Indicator
Possible security breach

Kill Chain Stage
Execute

Remediation Steps
Possible steps for further analysis/triage to consider:

1. Determine if the activity is approved by checking service management system for an incident / work order (ticket) associated with the activity.
2. Determine if the account has other anomalies.
3. Determine if the account or its peers have performed similar activities.
4. Determine if the account should be performing the activity via a role to privilege comparison.
5. Determine if the endpoint has other anomalies associated with its processes, sessions, or network connections.
6. Determine if any of the processes and their hash values are malicious.

Possible Remediation steps after further analysis and triage:

1. Submit a ticket to revert any changes that occurred.
2. Submit a ticket to disable the account.
3. Submit a ticket to remove the account (as needed)
4. Submit a ticket to revoke privileges
5. Submit a ticket to perform a full Antivirus scan
6. Submit a ticket for host isolation and further remediation as per internal IR playbooks dictate.

Detection Algorithm
Abnormal activity compared to peers

Criteria to Filter Event
baseeventid EQUAL TO 4657 [and]
Source Process Name CONTAINS regedit
AND
Account Name DOES NOT CONTAIN $ [and]
Account Name DOES NOT CONTAIN Anonymous [and]
Account Name DOES NOT CONTAIN LOCAL [and]
Account Name NOT EQUAL TO -

Verbose Info
Account: ${accountname!"ACCOUNTNAME"} IP address: ${ipaddress!"UNKNOWN"} Host: ${resourcename!"UNKNOWN"} Process Name:${sourceprocessname!"UNKNOWN"} Path: ${oldfilepath!"UNKNOWN"} Message: ${message!"UNKNOWN"} EventID: ${baseeventid!"UNKNOWN"}

Response Bot Fields/Attributes/Policies
Rare registry modification by an account
Suspicious Registry Modification Observed
Detection of possible backdoor

Rare Registry Modification by an Account

Criticality: Medium
Applies to: Functionality
Policy Category: Account Misuse

Device Category
Windows

Description
Rare registry modification attempts may be indicative of a possible circumvention of control activity or a malicious presence on the endpoint

Analytical Type
Tier 2 Behavior Summary

Technique Used
Behavior anomaly on registry modification activity

Prerequisites
- windows logs
- Behavior profiles

Violation Entity
Resource Group Account

Threat Focus Area
Insider/Cyber

Threat Indicator
Circumvention of controls

Kill Chain Stage
Recon

Remediation Steps
- VirusTotal ScanIP
- VirusTotal ScanURL
- VirusTotal ScanDomain
- Nessus LaunchScan
- NessusConnector StopScan
- NessusConnector FetchScan
- AD BlockUser
- AD UnBlockUser
- Tanium - Machine Information
- Tanium - Running Processes with MD5
- Tanium - Running Applciations
- Tanium - Non-approved Established Connections
- PassiveTotal - Get Passive DNS
- PassiveTotal - Get Subdomains
- PassiveTotal - Get Unique DNS
- PassiveTotal - Get Who Is
- PassiveTotal - Search Who is
- PassiveTotal - Search Who is by Keyword

Detection Algorithm
Rare behavior

Criteria to Filter Event
baseeventid EQUAL TO 4657
AND
Account Name NOT EQUAL TO - [and]
Account Name DOES NOT CONTAIN ANONYMOUS [and]
Account Name DOES NOT CONTAIN LOCAL [and]
Account Name DOES NOT CONTAIN $

Risk Boosters
Active List:
accountname in suspicious_host_accessed [and/or]
employeeid in:
- Possible_bruteforce
- suspicious_process_anomaly
- suspicious_AD_authentication
- possible_privilege_misuse
- vulnerable_endpoints
- infected_endpoints
increase factor 4.0

Verbose Info
Account: ${accountname!"ACCOUNTNAME"} IP address: ${ipaddress!"UNKNOWN"} Host: ${resourcename!"UNKNOWN"} Object Type:${devicecustomstring4!"UNKNOWN"} Object Value Name: ${devicecustomstring3!"UNKNOWN"}Object Name: ${deviecustomstring2!"UNKNOWN"} Message: ${message!"UNKNOWN"} EventID: ${baseeventid!"UNKNOWN"}

Response Bot Fields/Attributes/Policies
Rare regedit usage compared to peer
Suspicious Registry Modification Observed
Detection of possible backdoor

Rare Target Account Authentication Using Explicit Credentials
Criticality: None
Applies to: Functionality
Policy Category: Account Misuse

Device Category
Windows

Description
Rare target account during explicit credentials, could indicate a malicious entity attempting to impersonate as another account using elevated privileges.

Analytical Type
Tier 2 Behavior Summary

Technique Used
Behavior anomaly for rarity on target account

Prerequisites
- windows logs
- Behavior profiles

Violation Entity
Resource Group Account

Threat Focus Area
Insider/Cyber

Threat Indicator
Suspicious AD Authentication

Kill Chain Stage
Recon

Remediation Steps
- AD BlockUser
- AD UnBlockUser
- Tanium - Machine Information
- Tanium - Running Processes with MD5
- Tanium - Running Applciations
- Tanium - Non-approved Established Connections

Detection Algorithm
Rare behavior

Criteria to Filter Event
baseeventid EQUAL TO 4648 [and]
Account Name DOES NOT CONTAIN $ [and]
Account Name DOES NOT CONTAIN - [and]
Account Name DOES NOT CONTAIN LOCAL [and]
Account Name DOES NOT CONTAIN ANONYMOUS

Verbose Info
Account: ${accountname!"ACCOUNTNAME"} IP address: ${ipaddress!"UNKNOWN"} Host: ${resourcename!"UNKNOWN"} Destination User: ${destinationusername!"UNKNOWN"} Message: ${message!"UNKNOWN"} EventID: ${baseeventid!"UNKNOWN"}

Response Bot Fields/Attributes/Policies
Use of explicit credentials - Account sharing or Password misuse
Abnormal number of process execution using explicit credentials
Rare process detected for authentication using explicit credentials

---

Scheduled Task Creation
Criticality: Low
Applies to: Functionality
Policy Category: Account Misuse

Device Category
Windows

Description

Detects when tasks are scheduled. Scheduled tasks should be monitored as they can indicate an attacker creating persistence or an insider threat scheduling a task to occur.

Analytical Type
Tier 2 Behavior Summary

Prerequisites
- windows logs
- Behavior profiles

Violation Entity
Resource Group Account

Threat Focus Area
Insider/Cyber

Threat Indicator
Suspicious process execution

Kill Chain Stage
Execute

Remediation Steps
- Nessus LaunchScan
- NessusConnector StopScan
- NessusConnector FetchScan
- AD BlockUser
- AD UnBlockUser
- Tanium - Machine Information
- Tanium - Running Processes with MD5
- Tanium - Running Applciations
- Tanium - Non-approved Established Connections

Detection Algorithm
Spike in number of occurences

Criteria to Filter Event
baseeventid EQUAL TO 4698

Verbose Info
Account ${accountname!"ACCOUNTNAME"} performed ${transactionstring1!"ACTIVITY"} from ipaddress ${ipaddress!"UNKNOWN"}

Response Bot Fields/Attributes/Policies
Rare process creation on an endpoint
Rare token elevation for process
Rare process spawned by a parent process
Rare process detected for authentication using explicit credentials

Service Account Performing Interactive Logon
Criticality: None
Applies to: Functionality
Policy Category: Account Misuse

Device Category
Windows

Description
Service accounts are typically only used for batched or application tasks. Interactive logon from these accounts could indicate a potential misuse or bypass of controls

Analytical Type
Real Time Policy

Prerequisites
- windows logs

Violation Entity
Resource Group Account

Threat Focus Area
Insider/Cyber

Threat Indicator
Interactive logon by service accounts

Kill Chain Stage
Recon

Remediation Steps
- AD BlockUser
- AD UnBlockUser
- Tanium - Machine Information
- Tanium - Running Processes with MD5
- Tanium - Running Applciations
- Tanium - Non-approved Established Connections

Detection Algorithm
Individual event analytics

Criteria to Filter Event
baseeventid EQUAL TO 4624 [or]
baseeventid EQUAL TO 528 [or]
baseeventid EQUAL TO 540
AND
CustomNumber 1 EQUAL TO 2.0 [or]
CustomNumber 1 EQUAL TO 10.0 [or]
CustomNumber 1 EQUAL TO 11.0
AND
Account Name CONTAINS svc [or]
Account Name CONTAINS SRV

Verbose Info
Account: ${accountname!"ACCOUNTNAME"} IP address: ${ipaddress!"UNKNOWN"} Host: ${resourcename!"UNKNOWN"} Message: ${message!"UNKNOWN"} EventID: ${baseeventid!"UNKNOWN"}

Response Bot Fields/Attributes/Policies

Rare interactive logon by service account
High Number of Failed Logins from an Undocumented Account
VPN activity by undocumented accounts

Suspicious Account Activity–Kerberoasting–Peak TGS Request for User Analytic

Criticality: Low
Applies to: Functionality
Policy Category: Account Misuse

Device Category

Windows

Description

This event is an indication of an attacker collecting Kerberos Service Tickets for decryption to impersonate the embedded service accounts.

Analytical Type

Tier 2 Behavior Summary

Prerequisites

- windows logs

Violation Entity

Network Address

Threat Focus Area

Cyber

Threat Indicator

Suspicious Authentication

Kill Chain Stage

Recon

Remediation Steps

Possible steps for further analysis / triage to consider:

1. Determine if the referenced Service Account (Resource, if listed) has any anomalies.
2. Determine if the account has other anomalies.
3. Determine if the endpoint has other anomalies associated with its processes, sessions, or network connections.

Possible Remediation steps after further analysis and triage:

1. Submit a ticket to reset the service account password.
2. Submit a ticket to disable the source account or service account (as needed).
3. Submit a ticket to scan host for vulnerabilities &/or malware (as needed).
4. Open an investigation as per internal IR playbook dictates.

Detection Algorithm

Enumeration behavior

Criteria to Filter Event
baseeventid EQUAL TO 4769 [and]
Account Name NOT EQUAL TO krbtgt [and]
Account Name DOES NOT CONTAIN $

Verbose Info
Account ${accountname!"ACCOUNTNAME"} performed ${transactionstring1!"ACTIVITY"} from ipaddress ${ipaddress!"UNKNOWN"}

Response Bot Fields/Attributes/Policies
Password hash access
Suspicious Account Activity - Kerberoasting - Rare TGS Encryption Type For User Analytic
Suspicious Account Activity - Potential pass-the-hash - Host Length Analytic
Suspicious Account Activity - Potential pass-the-hash - Key Length Analytic
Suspicious Account Activity - Peak Credential Validation Failure Increase For Host Analytic
Suspicious Process Activity - Potential Mimikatz or Hash Passing Token Creation - Powershell Privileged Service Call Analytic
Suspicious Process Activity - Endpoint - Potential Mimikatz Object Handling Activity Analytic

---

Suspicious Account Activity– Kerberoasting–Rare TGS Encryption Type for User Analytic
Criticality: Low
Applies to: Functionality
Policy Category: Account Misuse

Device Category
Windows

Description
Detects a rare service ticket granted encryption usage.

Analytical Type
Tier 2 Behavior Summary

Prerequisites
- windows logs
- Behavior profiles

Violation Entity
Network Address

Threat Focus Area
Cyber

Threat Indicator
Suspicious Authentication

Kill Chain Stage
Recon

Remediation Steps

Possible steps for further analysis/triage to consider:

1. Determine if the referenced Service Account (Resource, if listed) has any anomalies.
2. Determine if the account has other anomalies.
3. Determine if the endpoint has other anomalies associated with its processes, sessions, or network connections.

Possible Remediation steps after further analysis and triage:

1. Submit a ticket to reset the service account password.
2. Submit a ticket to disable the source account or service account (as needed).
3. Submit a ticket to scan host for vulnerabilities &/or malware (as needed).
4. Open an investigation as per internal IR playbook dictates.

Detection Algorithm

Rare behavior

Criteria to Filter Event

baseeventid EQUAL TO 4769 [and]
Account Name NOT EQUAL TO krbtgt [and]
Account Name DOES NOT CONTAIN $ [and]
devicecustomstring1 EQUAL TO 0x40810000
AND
devicecustomstring2 EQUAL TO 0x1 [and]
devicecustomstring2 EQUAL TO 0x2 [and]
devicecustomstring2 EQUAL TO 0x3 [and]
devicecustomstring2 EQUAL TO 0x17

Verbose Info

Account ${accountname!"ACCOUNTNAME"} performed ${transactionstring1!"ACTIVITY"} from ipaddress ${ipaddress!"UNKNOWN"}

Response Bot Fields/Attributes/Policies

Suspicious Account Activity - Kerberoasting - Peak TGS Request For User Analytic
Suspicious Process Activity - Potential Mimikatz or Hash Passing Token Creation - Powershell Privileged Service Call Analytic
Suspicious Account Activity - Potential pass-the-hash - Key Length Analytic
Suspicious Account Activity - Potential pass-the-hash - Host Length Analytic

---

Suspicious Account Activity–Peak Credential Validation Failure Increase for Host Analytic

Criticality: Low
Applies to: Functionality
Policy Category: Account Misuse

Device Category

Windows

Description

Detects spike in enumeration of accounts with failed login from a single host as compared to its daily profile

Analytical Type

Tier 2 Behavior Summary

Prerequisites
- windows logs
- Behavior profiles

Violation Entity
Resources

Threat Focus Area
Cyber

Threat Indicator
Suspicious Authentication

Kill Chain Stage
Recon

Remediation Steps
Possible steps for further analysis / triage to consider:

1. Determine if the activity is approved by checking service management system for an incident / work order (ticket) associated with the activity.
2. Determine if the source account has other anomalies.
3. Determine if the source account or its peers have performed similar activities.
4. Determine if the source account should be performing the activity via a role to privilege comparison.
5. Determine if the endpoint has other anomalies associated with its processes, sessions, or network connections.

Possible Remediation steps after further analysis and triage:

1. Submit a ticket to revert any changes made.
2. Submit a ticket to disable the account(s).
3. Submit a ticket to remove the account(s) (as needed)
4. Submit a ticket to revoke privileges
5. Open an investigation as per internal IR playbook dictates.

Detection Algorithm
Enumeration behavior

Criteria to Filter Event
baseeventid EQUAL TO 4776 [and]
eventoutcome EQUAL TO AUDIT_FAILURE

Verbose Info
Account ${accountname!"ACCOUNTNAME"} performed ${transactionstring1!"ACTIVITY"} from ipaddress ${ipaddress!"UNKNOWN"}

Response Bot Fields/Attributes/Policies
Abnormal number of failed logons on a resource- SIEM-13
High number of accounts used on a workstation for successful authentications or run as events
High number of accounts from the same ipaddress for successful authentications or run as events
High number of accounts from the same ipaddress for authentication failures or lockout events
Suspicious Account Activity - Peak Explicit Credentials Distinct Account Name For Host Analytic

Suspicious Account Activity–Peak Explicit Credentials Distinct Account Name for Host Analytic

Criticality: Low
Applies to: Functionality
Policy Category: Account Misuse

Device Category
Windows

Description
Detects spike in enumeration of accounts with failed login from a single host as compared to its daily profile

Analytical Type
Tier 2 Behavior Summary

Prerequisites
- windows logs
- Behavior profiles

Violation Entity
Resource Group Account

Threat Focus Area
Cyber

Threat Indicator
Possible account sharing or password misuse

Kill Chain Stage
Recon

Remediation Steps
- Nessus LaunchScan
- NessusConnector StopScan
- NessusConnector FetchScan
- AD BlockUser
- AD UnBlockUser
- Tanium - Machine Information
- Tanium - Running Processes with MD5
- Tanium - Running Applciations
- Tanium - Non-approved Established Connections

Detection Algorithm
Enumeration behavior

Criteria to Filter Event
baseeventid EQUAL TO 4648
AND
Account Name DOES NOT CONTAIN Destination User Name [and]
Destination User Name DOES NOT CONTAIN Account Name [and]
Account Name DOES NOT CONTAIN $ [and]
Account Name NOT EQUAL TO -

Verbose Info

Account ${accountname!"ACCOUNTNAME"} performed ${transactionstring1!"ACTIVITY"} from ipaddress ${ipaddress!"UNKNOWN"}

Response Bot Fields/Attributes/Policies

Abnormal object or network share access attempts by resource-SIEM-13
Abnormal number of failed logons on a resource- SIEM-13
Use of explicit credentials - Account sharing or Password misuse
High number of accounts used on a workstation for successful authentications or run as events
High number of accounts from the same ipaddress for successful authentications or run as events
High number of accounts from the same ipaddress for authentication failures or lockout events
Possible password spraying from a resource
Suspicious Account Activity - Peak Credential Validation Failure Increase For Host Analytic

---

Suspicious Account Activity–Potential Pass-the-Hash–Host Length Analytic

Criticality: Medium
Applies to: Functionality
Policy Category: Account Misuse

Device Category

Windows

Description

Detects rare potential pass the hash via host length events

Analytical Type

Tier 2 Behavior Summary

Prerequisites

- windows logs
- Behavior profiles

Violation Entity

Resource Group Account

Threat Focus Area

Cyber

Threat Indicator

Suspicious AD Authentication

Kill Chain Stage

Recon

Remediation Steps

- AD BlockUser
- AD UnBlockUser
- Tanium - Machine Information
- Tanium - Running Processes with MD5
- Tanium - Running Applciations
- Tanium - Non-approved Established Connections

Detection Algorithm
Rare behavior

Criteria to Filter Event
Destination HostName DOES NOT CONTAIN DC [and]
baseeventid EQUAL TO 4776 [and]
Destination HostName IS NOT NULL [and]
Destination HostName DOES NOT CONTAIN - [and]
CustomNumber 3 EQUAL TO 16

Verbose Info
Account ${accountname!"ACCOUNTNAME"} performed ${transactionstring1!"ACTIVITY"} from ipaddress ${ipaddress!"UNKNOWN"}

Response Bot Fields/Attributes/Policies
Password hash access
Suspicious Account Activity - Potential pass-the-hash - Key Length Analytic
Suspicious Account Activity - Kerberoasting - Rare TGS Encryption Type For User Analytic
Suspicious Account Activity - Kerberoasting - Peak TGS Request For User Analytic
Suspicious Process Activity - Potential Mimikatz or Hash Passing Token Creation - Powershell Privileged Service Call Analytic
Pass the hash detection - Key length analysis
Pass the hash detection - Randomly generated hosts
Suspicious Process Activity - Endpoint - Potential Mimikatz Object Handling Activity Analytic

Suspicious Account Activity–Potential Pass-the-Hash–Key Length Analytic
Criticality: Medium
Applies to: Functionality
Policy Category: Account Misuse

Device Category
Windows

Description
Detects potential pass the hash via key-length

Analytical Type
Real Time Policy

Prerequisites
- windows logs

Violation Entity
Resource Group Account

Threat Focus Area
Cyber

Threat Indicator
Suspicious Authentication

Kill Chain Stage
Recon

Remediation Steps
Possible steps for further analysis / triage to consider:

1. Determine if the account has other anomalies.
2. Determine if the account should be performing the activity via a role to privilege comparison.
3. Determine if the endpoint has other anomalies associated with its processes, sessions, or network connections.

Possible Remediation steps after further analysis and triage:

1. Submit a ticket to disable the source account.
2. Submit a ticket to reset the password of the account whose hash was accessed.
3. Submit a ticket to scan host for vulnerabilities & malware (As Needed)
4. Open an investigation as per internal IR playbook dictates.

Detection Algorithm
Individual event analytics

Criteria to Filter Event
baseeventid EQUAL TO 4624 [or]
baseeventid EQUAL TO 4625
AND
Destination Process Name CONTAINS NtLmSsp [and]
CustomNumber 1 EQUAL TO 3 [and]
Account Name NOT EQUAL TO ANONYMOUS LOGON [and]
TransactionNumber 1 EQUAL TO 0

Verbose Info
Account ${accountname!"ACCOUNTNAME"} performed ${transactionstring1!"ACTIVITY"} from ipaddress ${ipaddress!"UNKNOWN"}

Response Bot Fields/Attributes/Policies
Password hash access
Suspicious Account Activity - Potential pass-the-hash - Host Length Analytic
Suspicious Account Activity - Kerberoasting - Rare TGS Encryption Type For User Analytic
Suspicious Account Activity - Kerberoasting - Peak TGS Request For User Analytic
Suspicious Process Activity - Potential Mimikatz or Hash Passing Token Creation - Powershell Privileged Service Call Analytic
Suspicious Process Activity - Endpoint - Potential Mimikatz Object Handling Activity Analytic
Pass the hash detection - Key length analysis
Pass the hash detection - Randomly generated hosts

Suspicious AD Enumeration Observed
Criticality: Low
Applies to: Functionality
Policy Category: Account Misuse

Device Category
Windows

Description
Detects security enabled local group enumeration

Analytical Type
Real Time Policy

Prerequisites
- windows logs

Violation Entity
Resource Group Account

Threat Focus Area
Cyber

Threat Indicator
Possible privilege enumeration

Kill Chain Stage
Exploit

Remediation Steps
- Nessus LaunchScan
- NessusConnector StopScan
- NessusConnector FetchScan
- AD BlockUser
- AD UnBlockUser
- Tanium - Machine Information
- Tanium - Running Processes with MD5
- Tanium - Running Applciations
- Tanium - Non-approved Established Connections

Detection Algorithm
Spotter

Criteria to Filter Event
resourcegroupname = "Microsoft Windows Events" and baseeventid=4799 and accountname=rmurphy

Verbose Info
Account: ${accountname!"ACCOUNTNAME"} IP address: ${ipaddress!"UNKNOWN"} Host: ${resourcename!"UNKNOWN"} Destination User: ${destinationusername!"UNKNOWN"} Message: ${message!"UNKNOWN"} EventID: ${baseeventid!"UNKNOWN"}

Response Bot Fields/Attributes/Policies
Possible remote interactive logon enumeration
Possible AD Enumeration
Abnormal number of accounts enumerated
Abnormal number of privileges enumerated
Rare account enumeration event
Rare privilege enumeration event
Abnormal number of account enumeration attempts on an endpoint
Possible Privilege Enumeration

Suspicious AD Policy Change
Criticality: None
Applies to: Functionality

Policy Category: Account Misuse

Device Category
Windows

Description
Detects a change in AD policy by an account

Analytical Type
Tier 2 Behavior Summary

Prerequisites
- windows logs
Behavior profiles

Violation Entity
Resource Group Account

Threat Focus Area
Insider/Cyber

Threat Indicator
Possible privilege misuse

Kill Chain Stage
Delivery

Remediation Steps
- AD BlockUser
- AD UnBlockUser
- Tanium - Machine Information
- Tanium - Running Processes with MD5
- Tanium - Running Applciations
- Tanium - Non-approved Established Connections

Detection Algorithm
Rare behavior

Criteria to Filter Event
baseeventid EQUAL TO 4713 [or]
baseeventid EQUAL TO 4714

Verbose Info
Account ${accountname!"ACCOUNTNAME"} performed ${transactionstring1!"ACTIVITY"} from ipaddress ${ipaddress!"UNKNOWN"}

Response Bot Fields/Attributes/Policies
Audit policy changes
Rare registry modification by an account
Rare regedit usage compared to peer

Suspicious Executables on a Machine

Criticality: None
Applies to: Functionality
Policy Category: Account Misuse

Device Category
Windows

Description
Detects a suspicious executable process started on a host

Analytical Type
Real Time Policy

Prerequisites
- windows logs

Violation Entity
Resource Group Account

Threat Focus Area
Cyber

Threat Indicator
Lateral movement

Kill Chain Stage
Execute

Remediation Steps
- AD BlockUser
- AD UnBlockUser
- Tanium - Machine Information
- Tanium - Running Processes with MD5
- Tanium - Running Applciations
- Tanium - Non-approved Established Connections

Detection Algorithm
Individual event analytics

Criteria to Filter Event
baseeventid EQUAL TO 4688
AND
Destination Process Name CONTAINS psexec.exe [or]
Destination Process Name CONTAINS mimikatz.exe [or]
Destination Process Name EQUAL TO metasploit.exe [or]
Source Process Name CONTAINS psexec.exe [or]
Source Process Name CONTAINS mimikatz.exe [or]
Source Process Name CONTAINS metasploit.exe [or]
Source Process Name CONTAINS net.exe [or]
Source Process Name CONTAINS powershell.exe [or]
Source Process Name CONTAINS at.exe [or]
Source Process Name CONTAINS psexecsvc.exe [or]
Destination Process Name CONTAINS powershell.exe [or]

Destination Process Name CONTAINS net.exe [or]
Destination Process Name CONTAINS psexecsvc.exe [or]
Destination Process Name CONTAINS at.exe

Verbose Info
Account ${accountname!"ACCOUNTNAME"} performed ${transactionstring1!"ACTIVITY"} from ipaddress ${ipaddress!"UNKNOWN"}

Response Bot Fields/Attributes/Policies
Rare process creation on an endpoint
Rare token elevation for process
Rare process spawned by a parent process
Rare process detected for authentication using explicit credentials
Suspicious Process Activity - Potential Mimikatz or Hash Passing Token Creation - Powershell Privileged Service Call Analytic
Suspicious Process Activity - Endpoint - Potential Mimikatz Object Handling Activity Analytic
Unusual service authentication detected for user
Suspicious Service creation
Rare service created on endpoint
Rare Basic Service Operation
Use of credential dumpers

Suspicious Host Access Behavior from an Account
Criticality: None
Applies to: Functionality
Policy Category: Account Misuse

Device Category
Windows

Description
Detects when a user attempts access multiple hosts as compared to the user's daily profile

Analytical Type
Tier 2 Behavior Summary

Prerequisites
- windows logs
Behavior profiles

Violation Entity
Resource Group Account

Threat Focus Area
Cyber

Threat Indicator
Lateral movement

Kill Chain Stage
Execute

Remediation Steps

- AD BlockUser
- AD UnBlockUser
- Tanium - Machine Information
- Tanium - Running Processes with MD5
- Tanium - Running Applciations
- Tanium - Non-approved Established Connections

Detection Algorithm
Enumeration behavior

Criteria to Filter Event
baseeventid EQUAL TO 4625 [or]
baseeventid EQUAL TO 4624 [or]
baseeventid EQUAL TO 4776

Verbose Info
Null

Response Bot Fields/Attributes/Policies
doneRare host accessed by an account
Rare host accessed by an account - Logon Success
Rare host accessed by an account - Logon Failure
Rare Host Accessed Attempt By Account
Rare Host Accessed from an Account

Suspicious Process Activity–Endpoint–Potential Mimikatz Object Handling Activity Analytic
Criticality: Low
Applies to: Functionality
Policy Category: Account Misuse

Device Category
Windows

Description
Generates a violation when mimkatz object handling is observed.

Analytical Type
Real Time Policy

Prerequisites
- windows logs

Violation Entity
Resource Group Account

Threat Focus Area
Cyber

Threat Indicator
Suspicious Access Pattern

Kill Chain Stage
Recon

Remediation Steps
- AD BlockUser
- AD UnBlockUser
- Tanium - Machine Information
- Tanium - Running Processes with MD5
- Tanium - Running Applciations
- Tanium - Non-approved Established Connections

Detection Algorithm
Individual event analytics

Criteria to Filter Event
baseeventid EQUAL TO 4656 [and]
devicecustomstring2 CONTAINS lsass [and]
devicecustomstring6 EQUAL TO 0x143a
AND
Destination Process Name CONTAINS mimikatz [or]
Source Process Name CONTAINS mimikatz

Verbose Info
Account ${accountname!"ACCOUNTNAME"} performed ${transactionstring1!"ACTIVITY"} from ipaddress ${ipaddress!"UNKNOWN"}

Response Bot Fields/Attributes/Policies
Possible AD Enumeration
Abnormal number of accounts enumerated
Abnormal number of privileges enumerated
Rare account enumeration event
Rare privilege enumeration event
Abnormal number of account enumeration attempts on an endpoint
Possible Privilege Enumeration
Suspicious AD Enumeration Observed
Suspicious Process Activity - Potential Mimikatz or Hash Passing Token Creation - Powershell Privileged Service Call Analytic
Suspicious Account Activity - Kerberoasting - Peak TGS Request For User Analytic
Suspicious Account Activity - Kerberoasting - Rare TGS Encryption Type For User Analytic
Suspicious Account Activity - Peak Credential Validation Failure Increase For Host Analytic
Suspicious Account Activity - Potential pass-the-hash - Key Length Analytic
Suspicious Account Activity - Potential pass-the-hash - Host Length Analytic
Rare process creation on an endpoint
Rare token elevation for process
Rare process spawned by a parent process
Rare logon process detected for windows authentication
Rare process detected for authentication using explicit credentials
Suspicious Process Activity - Log Clearing Analytics

Suspicious Registry Modification Observed
Criticality: Low
Applies to: Functionality
Policy Category: Account Misuse

Device Category

Windows

Description
Generates a violation when registry key value modifications are observed.

Analytical Type
Real Time Policy

Prerequisites
- windows logs

Violation Entity
Resource Group Account

Threat Focus Area
Cyber

Threat Indicator
Possible privilege misuse

Kill Chain Stage
Delivery

Remediation Steps
- AD BlockUser
- AD UnBlockUser
- Tanium - Machine Information
- Tanium - Running Processes with MD5
- Tanium - Running Applciations
- Tanium - Non-approved Established Connections

Detection Algorithm
Individual event analytics

Criteria to Filter Event
baseeventid EQUAL TO 4673 [and]
Account Name CONTAINS admin [and]
Destination User Privileges CONTAINS SeTcbPrivilege
AND
Source Process Name CONTAINS powershell [or]
Destination Process Name CONTAINS powershell

Verbose Info
Account ${accountname!"ACCOUNTNAME"} performed ${transactionstring1!"ACTIVITY"} from ipaddress ${ipaddress!"UNKNOWN"}

Response Bot Fields/Attributes/Policies
Use of credential dumpers
Rare process detected for authentication using explicit credentials
Rare token elevation for process
Rare process creation on an endpoint
Abnormal number of Kerberos impersonation attempts detected -13
Possible AD Enumeration
Abnormal number of accounts enumerated

Abnormal number of privileges enumerated
Suspicious Service creation
Rare account enumeration event
Rare privilege enumeration event
Abnormal number of account enumeration attempts on an endpoint
Possible Impersonation Detected
Suspicious AD Enumeration Observed
Suspicious Account Activity - Potential pass-the-hash - Host Length Analytic
Suspicious Account Activity - Potential pass-the-hash - Key Length Analytic
Suspicious Account Activity - Kerberoasting - Rare TGS Encryption Type For User Analytic
Suspicious Account Activity - Kerberoasting - Peak TGS Request For User Analytic
Suspicious Process Activity - Endpoint - Potential Mimikatz Object Handling Activity Analytic
Pass the hash detection - Key length analysis
Pass the hash detection - Randomly generated hosts
Suspicious executables on a machine

Suspicious Service Creation

Criticality: High
Applies to: Functionality
Policy Category: Account Misuse

Device Category

Windows

Description

This policy determines a user running a process/service on their machine not seen before

Analytical Type

Tier 2 Behavior Summary

Prerequisites

- windows logs

Violation Entity

Activity Account

Threat Focus Area

Cyber

Threat Indicator

Suspicious process execution

Kill Chain Stage

Execute

Remediation Steps

- Nessus LaunchScan
- NessusConnector StopScan
- NessusConnector FetchScan
- AD BlockUser
- AD UnBlockUser
- Tanium - Machine Information
- Tanium - Running Processes with MD5

- Tanium - Running Applciations
- Tanium - Non-approved Established Connections

Detection Algorithm
Spotter

Criteria to Filter Event
resourcename = IRCDPCTXMXA7 and accountname = Administrator and baseeventid = 4657

Verbose Info
Account: ${accountname!"ACCOUNTNAME"} IP address: ${ipaddress!"UNKNOWN"} Host: ${resourcename!"UNKNOWN"} Destination User: ${destinationusername!"UNKNOWN"} Message: ${message!"UNKNOWN"} EventID: ${baseeventid!"UNKNOWN"}

Response Bot Fields/Attributes/Policies
Audit policy changes
Rare registry modification by an account
Rare regedit usage compared to peer
Rare audit log clearing by an account
Firewall disabled on windows
Suspicious Service creation
Rare service created on endpoint
Rare Basic Service Operation
Rare process spawned by a parent process
Firewall configurations modified on windows
Scheduled Task Creation

Use of Explicit Credentials–Account Sharing or Password Misuse
Criticality: Low
Applies to: Functionality
Policy Category: Account Misuse

Device Category
Windows

Description
Explicit usage of another user's credentials could indicate a account takeover or a password sharing activity

Analytical Type
Real Time Policy

Prerequisites
- windows logs

Violation Entity
Resource Group Account

Threat Focus Area
Insider/Cyber

Threat Indicator
Possible account sharing or password misuse

Kill Chain Stage
Recon

Remediation Steps
- Nessus LaunchScan
- NessusConnector StopScan
- NessusConnector FetchScan
- AD BlockUser
- AD UnBlockUser
- Tanium - Machine Information
- Tanium - Running Processes with MD5
- Tanium - Running Applciations
- Tanium - Non-approved Established Connections
- Tanium - User Sessions

Detection Algorithm
Individual Event Analytics

Criteria to Filter Event
baseeventid EQUAL TO 4648
AND
Destination User Name NOT EQUAL TO [and]
Destination User Name NOT EQUAL TO Account Name [and]
u_id NOT EQUAL TO -1 [and]
Destination User Name DOES NOT CONTAIN User ID [and]
User ID DOES NOT CONTAIN Destination User Name [and]
Destination User Name DOES NOT CONTAIN Account Name [and]
Account Name DOES NOT CONTAIN Destination User Name
AND
Account Name NOT EQUAL TO - [and]
Account Name DOES NOT CONTAIN $ [and]
Account Name DOES NOT CONTAIN ANONYMOUS [and]
Account Name DOES NOT CONTAIN LOCAL

Verbose Info
Account: ${accountname!"ACCOUNTNAME"} IP address: ${ipaddress!"UNKNOWN"} Host: ${destinationhostname!"UNKNOWN"} Destination User: ${destinationusername!"UNKNOWN"} Message: ${message!"UNKNOWN"} EventID: ${baseeventid!"UNKNOWN"}

Response Bot Fields/Attributes/Policies
Abnormal number of account lockouts-SIEM-13
Abnormal number of remote interactive logon from an account-SIEM-13
Abnormal number of logon failures from an account-SIEM-13
Abnormal number of failed logons on a resource- SIEM-13
Rare host accessed by an account
Rare admin share access by an account
Rare interactive logon by service account
Rare host accessed by an account - Logon Success
Rare host accessed by an account - Logon Failure
Rare Host Accessed Attempt By Account
Remote interactive logon to domain controller by non-admin account
Rare Host Accessed from an Account
Suspicious Account Activity - Peak Explicit Credentials Distinct Account Name For Host Analytic
Rare object access attempts by an account
Rare logon type detected for an account

Abnormal Number of Failed SSH Authentication Attempts–Activity Account

Criticality: Low
Applies to: Functionality
Policy Category: Account Misuse

Device Category

Unix

Description

This is a behavior-based policy that detects spike in the number of failed SSH logins for a particular account

Analytical Type

Tier 2 Behavior Summary

Violation Entity

Activity Account

Threat Focus Area

Cyber

Threat Indicator

Spike In Failed SSHD Logs

Kill Chain Stage

Recon

Criteria to Filter Event

Device Action EQUAL TO authentication failure OR
Device Action EQUAL TO Failed password OR
Device Action EQUAL TO Invalid credentials
AND
requestclientapplication EQUAL TO sshd

Verbose Info

'Destination Host: ${destinationhostname!"Unknown"} Source IP: ${sourceaddress!"Unknown"} SessionID: ${sessionid!"Unknown"} ipaddress:${ipaddress!"UNKNOWN"} Action:${deviceaction!"Unknown"} Application: ${requestclientapplication!"Unknown"} Destination port: ${destinationport!"Unknown"}'

Response Bot Fields/Attributes/Policies

deviceaction,requestclientapplication,destinationhostname,destinationport,sourceusername,sourceip

Abnormal Number of Login Failures–SU

Criticality: Low
Applies to: Functionality
Policy Category: Account Misuse

Device Category

Unix

Description

This is a behavior-based policy that detects spike in the number of failed SU authentication logins for a particular account

Analytical Type
Tier 2 Behavior Summary

Violation Entity
Activity Account

Threat Focus Area
Cyber

Threat Indicator
Spike in SU authentication failures

Kill Chain Stage
Recon

Criteria to Filter Event
Device Action EQUAL TO password check failed
Device Action EQUAL TO authentication failure
Device Action EQUAL TO failed
AND
requestclientapplication EQUAL TO su

Verbose Info
Destination Host: ${destinationhostname!"Unknown"} Source IP: ${sourceaddress!"Unknown"} SessionID: ${sessionid!"Unknown"} ipaddress:${ipaddress!"UNKNOWN"} Action:${deviceaction!"Unknown"} Application: ${requestclientapplication!"Unknown"} Destination port: ${destinationport!"Unknown"}

Response Bot Fields/Attributes/Policies
deviceaction,requestclientapplication,destinationhostname,destinationport,sourceusername,sourceip

---

Activity on a Rare Hostname Never Connected Before
Criticality: Low
Applies to: Functionality
Policy Category: Account Misuse

Device Category
Unix

Description
This policy detects account logging on successfully to a host never connected before.

Analytical Type
Tier 2 Behavior Summary

Violation Entity
Activity Account

Threat Focus Area
Insider/Cyber

Threat Indicator
Activity towards a rare hostname never connected before

Kill Chain Stage
Exploit

Remediation Steps
N/A

Criteria to Filter Event
Device Action EQUAL TO session opened OR
Device Action EQUAL TO Accepted password OR
Device Action EQUAL TO Accepted publickey OR
Device Action EQUAL TO Login successful

Verbose Info
'Account ${accountname!"ACCOUNTNAME"} of employee ${u_employeeid!"Unknown"} terminated on ${u_terminationdate!"Unknown"} was detected performing activity on ${transactionstring1$LASTACCESSTIME!"Unknown"}'

Response Bot Fields/Attributes/Policies
deviceaction,requestclientapplication,destinationhostname,destinationport,sourceusername,sourceip

---

Activity Performed by Terminated Account
Criticality: Low
Applies to: Functionality
Policy Category: Account Misuse

Device Category
Unix

Description
This policy detects users performing activity post their termination

Analytical Type
IEE

Violation Entity
Activity Account

Threat Focus Area
Insider/Cyber

Threat Indicator
Activity by Terminated User

Kill Chain Stage
Recon

Criteria to Filter Event
STATUS EQUAL TO 0 AND
Event Time GREATER THAN TERMINATION DATE

Verbose Info

'Account ${accountname!"ACCOUNTNAME"} of employee ${u_employeeid!"Unknown"} terminated on ${u_terminationdate!"Unknown"} was detected performing activity on ${transactionstring1$LASTACCESSTIME!"Unknown"}'

Response Bot Fields/Attributes/Policies

deviceaction,requestclientapplication,destinationhostname,destinationport,sourceusername,sourceip

---

Detect Audit Log Tampering

Criticality: Low
Applies to: Functionality
Policy Category: Account Misuse

Device Category

Unix

Description

This policy detects unauthorized modifications to Unix log files

Analytical Type

IEE

Violation Entity

Activity Account

Threat Focus Area

Insider/Cyber

Threat Indicator

Audit Log Tampering

Kill Chain Stage

Execute

Criteria to Filter Event

devicecustomstring1 CONTAINS chown OR
devicecustomstring1 CONTAINS rm OR
devicecustomstring1 CONTAINS mv OR
devicecustomstring1 CONTAINS cat OR
devicecustomstring1 CONTAINS chmod OR
devicecustomstring1 CONTAINS setfacl OR
devicecustomstring1 CONTAINS chgrp OR

AND

devicecustomstring1 CONTAINS /var/log OR
devicecustomstring1 CONTAINS /var/messages OR
devicecustomstring1 CONTAINS /etc/security OR
devicecustomstring1 CONTAINS /etc/kshrc OR
devicecustomstring1 CONTAINS /etc/bashrc OR
devicecustomstring1 CONTAINS /etc/lgr OR

Verbose Info

'Destination Host: ${destinationhostname!"Unknown"} Source IP: ${sourceaddress!"Unknown"} Command: ${devicecustomstring1!"UNKNOWN"} SessionID: ${sessionid!"Unknown"} ipaddress:${ipaddress!"UNKNOWN"} Action:${deviceaction!"Unknown"} Application: ${requestclientapplication!"Unknown"}'

Response Bot Fields/Attributes/Policies

deviceaction,requestclientapplication,destinationhostname,destinationport,devicecustomstring1,sourceusername,sourceip

---

Detect Password Retrieval from System Files

Criticality: Low
Applies to: Functionality
Policy Category: Account Misuse

Device Category

Unix

Description

This policy detects accounts attempting to retrieve passwords from /etc/passwd and /etc/shadow files

Analytical Type

IEE

Violation Entity

Activity Account

Threat Focus Area

Insider/Cyber

Threat Indicator

Password Reset Anomaly

Kill Chain Stage

Exploit

Criteria to Filter Event

devicecustomstring1 CONTAINS cat OR
 devicecustomstring1 CONTAINS grep OR
 devicecustomstring1 CONTAINS vi OR
 devicecustomstring1 CONTAINS cp OR
 devicecustomstring1 CONTAINS scp OR
AND
devicecustomstring1 CONTAINS passwd
 devicecustomstring1 CONTAINS shadow

Verbose Info

'Destination Host: ${destinationhostname!"Unknown"} Source IP: ${sourceaddress!"Unknown"} SessionID: ${sessionid!"Unknown"} ipaddress:${ipaddress!"UNKNOWN"} Action:${deviceaction!"Unknown"} Application: ${requestclientapplication!"Unknown"} Destination port: ${destinationport!"Unknown"}'

Response Bot Fields/Attributes/Policies

deviceaction,requestclientapplication,destinationhostname,destinationport,devicecustomstring1,sourceusername,sourceip

Detect Presence and Attempted Use of the Telnet Utility

Criticality: Low
Applies to: Functionality
Policy Category: Account Misuse

Device Category
Unix

Description
This policy detects attempted use of the telnet utility

Analytical Type
IEE

Violation Entity
Activity Account

Threat Focus Area
Insider/Cyber

Threat Indicator
Detect presence and attempted use of the telnet utility

Kill Chain Stage
Exploit

Criteria to Filter Event
devicecustomstring contains telnet

Verbose Info
'Destination Host: ${destinationhostname!"Unknown"} Source IP: ${sourceaddress!"Unknown"} Command: ${devicecustomstring1!"UNKNOWN"} SessionID: ${sessionid!"Unknown"} ipaddress:${ipaddress!"UNKNOWN"} Action:${deviceaction!"Unknown"} Application: ${requestclientapplication!"Unknown"}'

Response Bot Fields/Attributes/Policies
deviceaction,requestclientapplication,destinationhostname,destinationport,devicecustomstring1,sourceusername,sourceip

Detect Use of XTERM, XWindows by User

Criticality: Low
Applies to: Functionality
Policy Category: Account Misuse

Device Category
Unix

Description
This policy detects accounts using XTerm/XWindows

Analytical Type
IEE

Violation Entity
Activity Account

Threat Focus Area
Insider/Cyber

Threat Indicator
Detect use of XTERM,Xwindows by user

Kill Chain Stage
Exploit

Criteria to Filter Event
devicecustomstring contains xterm

Verbose Info
Destination Host: ${destinationhostname!"Unknown"} Source IP: ${sourceaddress!"Unknown"} Command: ${devicecustomstring1!"UNKNOWN"} SessionID: ${sessionid!"Unknown"} ipaddress:${ipaddress!"UNKNOWN"} Action:${deviceaction!"Unknown"} Application: ${requestclientapplication!"Unknown"}

Response Bot Fields/Attributes/Policies
deviceaction,requestclientapplication,destinationhostname,destinationport,devicecustomstring1,sourceusername,sourceip

Successful Authentication to Multiple Destination Hosts in a Short Period of Time–Activity Account
Criticality: None
Applies to: Functionality
Policy Category: Account Misuse

Device Category
Unix

Description
This policy detects accounts performing successful SSH login from single source host to at least 5 destination hosts within a duration of one hour

Analytical Type
Directive

Violation Entity
Activity Account

Threat Focus Area
Insider/Cyber

Threat Indicator
Account connecting to multiple destination address\

Kill Chain Stage
Recon

Criteria to Filter Event
Device Action EQUAL TO session opened OR
Device Action EQUAL TO Accepted password OR
Device Action EQUAL TO Accepted publickey

Verbose Info
'Destination Host: ${destinationhostname!"Unknown"} Source IP: ${sourceaddress!"Unknown"} SessionID: ${sessionid!"Unknown"} ipaddress:${ipaddress!"UNKNOWN"} Action:${deviceaction!"Unknown"} Destination port: ${destinationport!"Unknown"} Application: ${requestclientapplication!"Unknown"}'

Response Bot Fields/Attributes/Policies
deviceaction,requestclientapplication,destinationhostname,destinationport,sourceusername,sourceip

---

User Emailing Files to External Email Addresses
Criticality: Low
Applies to: Functionality
Policy Category: Account Misuse

Device Category
Unix

Description
This policy detects users using mail service on Unix hosts to email externally

Analytical Type
IEE

Violation Entity
Activity Account

Threat Focus Area
Insider/Cyber

Threat Indicator
User emailing files to external email addresses

Kill Chain Stage
Exfiltration

Criteria to Filter Event
devicecustomstring1 contains mail and devicecustomstring1 contains @

Verbose Info
'Destination Host: ${destinationhostname!"Unknown"} Source IP: ${sourceaddress!"Unknown"} Command: ${devicecustomstring1!"UNKNOWN"} SessionID: ${sessionid!"Unknown"} ipaddress:${ipaddress!"UNKNOWN"} Action:${deviceaction!"Unknown"} Application: ${requestclientapplication!"Unknown"}'

Response Bot Fields/Attributes/Policies

deviceaction,requestclientapplication,destinationhostname,destinationport,devicecustomstring1,sourceusername,sourceip

---

Abnormal Number of Account Enumeration Attempts on an Endpoint

Criticality: Low
Applies to: Functionality
Policy Category: Malware

Device Category

Windows

Description

High number of accounts used during failed authentication events or lockout events may be indicative of malicious insider/cyber attempting to guess passwords for accounts.

Analytical Type

Tier 2 Behavior Summary

Technique Used

Enumeration Behavior anomaly for accounts used

Prerequisites

- windows logs
- Behavior profiles
- Peer correlation: Title / Department
- Client Naming conventions
- CMDB data

Violation Entity

Resources

Threat Focus Area

Cyber

Threat Indicator

Network Scanning and Enumeration

Kill Chain Stage

Recon

Remediation Steps

Possible further analysis/triage steps to consider:

1. Determine if the Source is a Virtual Desktop Server / SCCM server.
2. Determine if the host has any other anomalies/Look for processes run on this host

Possible Remediation steps after further analysis/triage:

1. Open ticket to add server to whitelist / Criteria to Filter event to stop future false positives.
2. If successful logins observed, Open ticket to Disable and reset password for accounts as they could be compromised.
3. If host found to be malicious, Open ticket to Isolate / remediate system according to internal Incident Response playbook.

Detection Algorithm

Enumeration Behavior
baseeventid, destinationhostname, transactionstring1
distinct destinationusername
Count of distinct accounts used during authentication failures
Self
Distinct transaction occurence abnormally highter than daily behavior for resoures
Sigma: 0.5

Criteria to Filter Event

baseeventid equal to 4625 [or]
AND
Account Name does not contain LOCAL [and]
Account name does not contain $ [and]
account Name does not contain ANONYMOUS [and]
Account name not equal to –

Verbose Info

IP address: ${ipaddress!"UNKNOWN"} with Host name: ${resourcename!"UNKNOWN"} enumerated Accounts: ${accountname$LIST!"ACCOUNTNAME"} Message: ${message!"UNKNOWN"} EventID: ${baseeventid!"UNKNOWN

Response Bot Fields/Attributes/Policies

Possible remote interactive logon enumeration
Rare account enumeration event
Abnormal number of account lockouts-SIEM-13
Abnormal number of remote interactive logon from an account-SIEM-13
Abnormal number of failed logons from an ipaddress-SIEM-13
Abnormal number of kerberos pre authentication failures-SIEM-13
Abnormal number of logon failures-SIEM-13
Abnormal number of remote logon attempts-SIEM-13
Abnormal number of logon failures from an account-SIEM-13
Abnormal number of failed logons on a resource- SIEM-13
Multiple failed logons
Possible password spraying from an ipaddress
Possible password spraying from a resource
Abnormal number of password resets
Abnormal number of accounts enumerated
Abnormal number of account lockout events
Abnormal number of kerberos pre authentication failures
High number of accounts from the same ipaddress for authentication failures or lockout events
Abnormal number of logon failures
Abnormal number of remote logon attempt
High Number of Failed Logins from an Undocumented Account

Possible Brute Force Attack VPN
Abnormal number of account lockouts-SIEM-17
Abnormal number of failed logons from an ipaddress-SIEM-17
Abnormal number of kerberos pre authentication failures-SIEM-17
Abnormal number of failed logons on a resource- SIEM-17

DISTCOUNT (destinationusername) - Count of unique accounts observed in violation

Abnormal Number of Kerberos Impersonation Attempts Detected–SIEM-13

Criticality: Low
Applies to: Functionality
Policy Category: Malware

Device Category

Windows

Description

This event is an indication of an attacker collecting Kerberos Service Tickets to impersonate the embedded service accounts.

Analytical Type

Directive Based

Prerequisites

- windows logs
- Account Naming conventions
- Host naming conventions

Violation Entity

Activity Account

Threat Focus Area

Cyber

Threat Indicator

Suspicious Network Traffic

Kill Chain Stage

Recon

Remediation Steps

Possible steps for further analysis / triage to consider:

1. Determine if the referenced Service Account (Resource, if listed) has any anomalies.
2. Determine if the account has other anomalies.
3. Determine if the endpoint has other anomalies associated with its processes, sessions, or network connections.

Possible Remediation steps after further analysis and triage:

1. Submit a ticket to reset the service account password.
2. Submit a ticket to disable the source account or service account (as needed).
3. Submit a ticket to scan host for vulnerabilities &/or malware (as needed).

4. Open an investigation as per internal IR playbook dictates.

Detection Algorithm

Aggregated event analytics

Criteria to Filter Event

baseeventid EQUAL TO 4769 [and]
Account Name DOES NOT CONTAIN filepath [and]
filepath NOT EQUAL TO krbtgt [and]
Account Name DOES NOT CONTAIN $ [and]
Account Name DOES NOT CONTAIN svc [and]
filepath DOES NOT CONTAIN LDAP [and]
Account Name DOES NOT CONTAIN LOCAL [and]
Account Name DOES NOT CONTAIN ANONYMOUS [and]
Account Name NOT EQUAL TO -

Directives

Name Total number of distinct file paths accessed
Filter for Events matching criteria? NA
Having similar accountname
Number of Occurrences 5
Within Duration 00:20:00
Should events happen consecutively? false
Distinct? filepath

Verbose Info

Account: ${accountname!"UNKNOWN"} requested Service Tickets for: ${filepath$LIST!"UNKNOWN"} from IP address: ${ipaddress!"UNKNOWN"} Message: ${message!"UNKNOWN"} EventID: ${baseeventid!"UNKNOWN"}

Response Bot Fields/Attributes/Policies

Abnormal number of kerberos pre authentication failures-SIEM-13
Abnormal object or network share access attempts by resource-SIEM-13
Abnormal number of remote interactive logon from an account-SIEM-13
Abnormal number of failed logons from an ipaddress-SIEM-13
Abnormal number of administrative share object accessed-SIEM-13
Abnormal number of hosts accessed-SIEM-13
Abnormal number of logon failures-SIEM-13
Abnormal object or network share access attempts-SIEM-13
Abnormal number of remote logon attempts-SIEM-13
Abnormal number of logon failures from an account-SIEM-13
Abnormal number of failed logons on a resource- SIEM-13
Abnormal number of service tickets requested-SIEM-13
Multiple failed logons
Possible password spraying from an ipaddress
Possible password spraying from a resource
Rare admin share access by an account
Abnormal number of network share object access
Abnormal number of kerberos pre authentication failures
Abnormal number of host access attempts
Abnormal number of hosts accessed
High number of accounts from the same ipaddress for authentication failures or lockout events
Abnormal number of administrative share object accessed
Rare host accessed by an account - Logon Success
Spike in administrative shares accessed
Rare host accessed by an account - Logon Failure

Rare Host Accessed Attempt By Account
Unusual high number of network shares accessed - SIEM
Abnormal number of remote logon attempts
Suspicious Account Activity - Kerberoasting - Rare TGS Encryption Type For User Analytic
Suspicious Account Activity - Kerberoasting - Peak TGS Request For User Analytic
Rare Host Accessed from an Account
Suspicious host access behavior from an account
Rare object access attempts by an account
Abnormal number of administrative share object accessed-SIEM-17
Abnormal number of hosts accessed-SIEM-17
Abnormal number of kerberos pre authentication failures-SIEM-17
Abnormal number of failed logons on a resource- SIEM-17
Abnormal number of Kerberos impersonation attempts detected -17
Abnormal number of failed logons from an ipaddress-SIEM-17
Abnormal number of remote logon attempt
Suspicious Logon Attempts
Abnormal number of logon failures

Abnormal Number of Kerberos Pre-Authentication Failures

Criticality: Low
Applies to: Functionality
Policy Category: Malware

Device Category

Windows

Description

Abnormal number of Kerberos pre-authentication failures could be indicative of a possible bruteforce event.

Technique Used

Behavior anomaly on the Kerberos pre authentication failures

Analytical Type

Tier 2 Behavior Summary

Prerequisites

- windows logs
- Behavior profiles

Violation Entity

Resource Group Account

Threat Focus Area

Cyber

Threat Indicator

Suspciious AD Authentication

Kill Chain Stage

Recon

Remediation Steps

Possible steps for further analysis / triage to consider:

1. Determine if the account has other anomalies.
2. Determine if the endpoints have other anomalies associated with their processes, sessions, or network connections.

Possible Remediation steps after further analysis and triage:

1. Submit a ticket to revert any changes that occurred.
2. Submit a ticket to reset password / disable the account.
3. Submit a ticket to remove the account (as needed)
4. Submit a ticket to isolate endpoints according to IR playbook

Detection Algorithm

Spike in Number of Occourences
Features: TransactionString1
Daily Kerberos pre authentication failures-9
Flagged Self
Transaction Occurence Abnormally Higher than users Daily behavior
Sigma 0.5

Criteria to Filter Event

baseeventid equal to 4771
AND
Account Name NOT EQUAL TO -
Account Name DOES NOT CONTAIN $
Account Name DOES NOT CONTAIN ANONYMOUS
Account Name DOES NOT CONTAIN LOCAL

Verbose Info

Account: ${accountname!"ACCOUNTNAME"} from IP address: ${ipaddress!"UNKNOWN"} Host: ${resourcename!"UNKNOWN"} had Message: ${message!"UNKNOWN"} EventID: ${baseeventid!"UNKNOWN"}

Response Bot Fields/Attributes/Policies

Abnormal number of Kerberos impersonation attempts detected-SIEM-13
Abnormal number of kerberos pre authentication failures-SIEM-13
Abnormal number of Kerberos impersonation attempts detected -17
Abnormal number of failed logons from an ipaddress-SIEM-13
Abnormal number of logon failures-SIEM-13
Abnormal number of remote logon attempts-SIEM-13
Abnormal number of logon failures from an account-SIEM-13
Abnormal number of failed logons on a resource- SIEM-13
Multiple failed logons
Abnormal number of logon failures
Suspicious Logon Attempts
Abnormal number of remote logon attempt
Rare host accessed by an account - Logon Failure
Abnormal number of remote logon attempts
Suspicious Account Activity - Kerberoasting - Rare TGS Encryption Type For User Analytic
Suspicious Account Activity - Kerberoasting - Peak TGS Request For User Analytic
Abnormal number of failed logons from an ipaddress-SIEM-17
Abnormal number of failed logons on a resource- SIEM-17

Abnormal Number of Logon Failures

Criticality: Low

Applies to: Functionality
Policy Category: Malware

Device Category
Windows

Description
Abnormal number of logon failures could be indicative of a possible account takeover attempt. Logon failure reason could further indicate the severity of this attack

Technique Used
Behavior anomaly on the logon failure activity for an account

Analytical Type
Tier 2 Behavior Summary

Prerequisites
- windows logs
- Behavior profiles
- Account naming convention if svc accounts are to be excluded

Violation Entity
Resource Group Account

Threat Focus Area
Cyber

Threat Indicator
Possible brute force

Kill Chain Stage
Recon

Remediation Steps
Possible further analysis/ triage steps to consider:

1. Determine if the target account has any other anomalies
2. Determine If there are any successful logins against the target account.
3. Determine if the Target account's peers have any anomalies associated.
4. Determine if there is a commonality between the resources, such as all belonging to one depart or specific set of users.
5. Determine if any of the sources has additional anomalies.

Possible Remediation steps after further analysis/triage:

1. If successful login observed, open ticket to disable and reset password for target account as it could be compromised.
2. If any host found to be malicious, Open ticket to Isolate / remediate system according to internal Incident Response playbook.

Notes:

- If screen for a service account check to see if a password was recently changed as scripts could be hardcoded with the password and were not updated to reflect the change and thus it triggered an alert.

- Check if the primary resource causing failed logins is a mobile device assigned to the user. the device may caused failed logins / lockouts if the password is not properly synced when changed by a user.

Detection Algorithm

baseeventid EQUAL TO 4625 [or]
baseeventid EQUAL TO 529 [or]
baseeventid EQUAL TO 530 [or]
baseeventid EQUAL TO 531 [or]
baseeventid EQUAL TO 532 [or]
baseeventid EQUAL TO 533 [or]
baseeventid EQUAL TO 534 [or]
baseeventid EQUAL TO 535 [or]
baseeventid EQUAL TO 536 [or]
baseeventid EQUAL TO 537 [or]
baseeventid EQUAL TO 539
AND
Account Name NOT EQUAL TO - [and]
Account Name DOES NOT CONTAIN $ [and]
Account Name DOES NOT CONTAIN ANONYMOUS [and]
Account Name DOES NOT CONTAIN LOCAL

Criteria to Filter Event

baseeventid equal to 4771
AND
Account Name NOT EQUAL TO -
Account Name DOES NOT CONTAIN $
Account Name DOES NOT CONTAIN ANONYMOUS
Account Name DOES NOT CONTAIN LOCAL

Risk Boosters

Match Criteria:
customstring 1 equal to 0xc000015b [or]
customstring 1 equal to 0xC000006A
increase factor 4.0

Verbose Info

Account: ${accountname!"ACCOUNTNAME"} had failed logins from IP addresses: ${ipaddress$LIST!"UNKNOWN"} with Host names: ${resourcename$LIST!"UNKNOWN"} Message: ${message!"UNKNOWN"} EventID: ${baseeventid!"UNKNOWN"}

Response Bot Fields/Attributes/Policies

Abnormal number of remote interactive logon from an account-SIEM-13
Abnormal number of failed logons from an ipaddress-SIEM-13
Abnormal number of logon failures-SIEM-13
Abnormal number of remote logon attempts-SIEM-13
Abnormal number of logon failures from an account-SIEM-13
Abnormal number of failed logons on a resource- SIEM-13
Multiple failed logons
Suspicious Logon Attempts
Abnormal number of remote logon attempt
Rare host accessed by an account - Logon Failure
Abnormal number of remote logon attempts
Abnormal number of failed logons from an ipaddress-SIEM-17
Abnormal number of failed logons on a resource- SIEM-17
Abnormal number of failed logins for an account
Abnormal number of kerberos pre authentication failures-SIEM-13
High Number of Failed Logins from an Undocumented Account

Abnormal Number of Network Share Object Access

Criticality: Low
Applies to: Functionality
Policy Category: Malware

Device Category

Windows

Description

A spike in account accessing new network objects may be indicative of a possible snooping or a recon activity

Technique Used

Behavior anomaly on the network share access activity

Analytical Type

Tier 2 Behavior Summary

Prerequisites

- windows logs
- Behavior profiles
- Host naming convention

Violation Entity

Resource Group Account

Threat Focus Area

Cyber

Threat Indicator

Suspicious network share access

Kill Chain Stage

Recon

Remediation Steps

Possible steps for further analysis / triage to consider:

1. Determine if the activity is approved by:
    - Checking service management system for an incident / work order (ticket) associated with the activity
    - Comparison to the user's peer group
    - Role to privilege comparison
2. Determine if the source account has other anomalies.
3. Determine if the endpoint has other anomalies associated with its processes, sessions, or network connections.

Possible Remediation steps after further analysis and triage:

1. Submit a ticket to revert any changes that occurred.
2. Submit a ticket to reset passwords / disable the account(s).
3. Submit a ticket to remove the account(s) (as needed)
4. Submit a ticket to revoke privileges
5. Submit a ticket to perform a full Antivirus scan
6. Submit a ticket for host isolation and further remediation as per internal IR playbooks dictate.

Detection Algorithm
Enumeration Behavior

Criteria to Filter Event
baseeventid EQUAL TO 5140 [and]
Account Name NOT EQUAL TO NA [and]
Account Name NOT EQUAL TO - [and]
Account Name DOES NOT CONTAIN $ [and]
Account Name DOES NOT CONTAIN ANONYMOUS [and]
Account Name DOES NOT CONTAIN LOCAL

Risk Boosters
Match Criteria:
baseeventid equal to 5140
increase factor 4.0

Verbose Info
Account: ${accountname!"ACCOUNTNAME"} IP address: ${ipaddress!"UNKNOWN"} Host: ${resourcename!"UNKNOWN"} Share Name: ${resourcecustomfield5!"UNKNOWN"} Message: ${message!"UNKNOWN"} EventID: ${baseeventid!"UNKNOWN"}

Response Bot Fields/Attributes/Policies
Abnormal object or network share access attempts by resource-SIEM-13
Abnormal object or network share access attempts-SIEM-13
Unusual high number of network shares accessed – SIEM

Abnormal Number of Process Execution Using Explicit Credentials
Criticality: Low
Applies to: Functionality
Policy Category: Malware

Device Category
Windows

Description
A spike in run-as activity may be indicative of an account that might be laterally propagating using other accounts and running processes using those accounts

Technique Used
Behavior anomaly on the usage of explicit credentials

Analytical Type
Tier 2 Behavior Summary

Prerequisites
- windows logs
- Behavior profiles
- user HR data
- user naming convention

- Host naming convention

Violation Entity
Resource Group Account

Threat Focus Area
Cyber

Threat Indicator
Suspicious Process execution

Kill Chain Stage
Execute

Remediation Steps
Possible steps for further analysis / triage to consider:

1. Determine if the activity is approved by:
    - Checking service management system for an incident / work order (ticket) associated with the activity
    - Comparison to the user's peer group
    - Role to privilege comparison
1. Determine if the target accounts have any anomalies
2. Determine if the source account has other anomalies.
3. Determine if the endpoint has other anomalies associated with its processes, sessions, or network connections.

Possible Remediation steps after further analysis and triage:

1. Submit a ticket to reset passwords / disable the account(s).
2. Submit a ticket to remove the account(s) (as needed)
3. Submit a ticket to revoke privileges
4. Submit a ticket to perform a full Antivirus scan
5. Submit a ticket for host isolation and further remediation as per internal IR playbooks dictate

Note:

- Desktop Support personnel commonly use "Run As" to execute tasks while completing service tickets.
- Service accounts generally carry out batch jobs that may also trigger this event from time to time.

Detection Algorithm
Spike in Number of Occourences

Criteria to Filter Event
baseeventid EQUAL TO 552 [or]
baseeventid EQUAL TO 4648
AND
Account Name DOES NOT CONTAIN $ [and]
Account Name NOT EQUAL TO - [and]
Account Name DOES NOT CONTAIN LOCAL [and]
Account Name DOES NOT CONTAIN ANONYMOUS

Risk Boosters
- criteria match

Destination User name contains Account Name increase factor 4.0

Verbose Info
Account: ${accountname!"ACCOUNTNAME"} IP address: ${ipaddress!"UNKNOWN"} Host: ${resourcename!"UNKNOWN"} Destination User: ${destinationusername!"UNKNOWN"} Message: ${message!"UNKNOWN"} EventID: ${baseeventid!"UNKNOWN"}

Response Bot Fields/Attributes/Policies
Rare process creation on an endpoint
Rare token elevation for process
Rare process spawned by a parent process
Rare logon process detected for windows authentication
Rare process detected for authentication using explicit credentials
Suspicious Process Activity - Log Clearing Analytics
Suspicious Process Activity - Potential Mimikatz or Hash Passing Token Creation - Powershell Privileged Service Call Analytic
Suspicious Process Activity - Endpoint - Potential Mimikatz Object Handling Activity Analytic

---

Abnormal Number of Remote Logon Attempts
Criticality: Low
Applies to: Functionality
Policy Category: Malware

Device Category
Windows

Description
This policy detects a spike in successful remote interactive logons which could indicate lateral movement

Analytical Type
Tier 2 Behavior Summary

Prerequisites
- windows logs
- Behavior profiles
- user HR data
- user naming convention
- Host naming convention

Violation Entity
Resource Group Account

Threat Focus Area
Cyber

Threat Indicator
Spike in remote interactive logon attempts

Kill Chain Stage
Recon

Remediation Steps
Possible steps for further analysis/triage to consider:

1. Determine if the activity is approved by:
    - Checking service management system for an incident / work order (ticket) associated with the activity
    - Comparison to the user's peer group
    - Role to privilege comparison
2. Determine if the target accounts have any anomalies
3. Determine if the source account has other anomalies.
4. Determine if the endpoint has other anomalies associated with its processes, sessions, or network connections.

Possible Remediation steps after further analysis and triage:

1. Submit a ticket to reset passwords / disable the account(s).
2. Submit a ticket to remove the account(s) (as needed)
3. Submit a ticket to revoke privileges
4. Submit a ticket to perform a full Antivirus scan
5. Submit a ticket for host isolation and further remediation as per internal IR playbooks dictate

Note:

- Desktop Support / Network Engineers / Administrators will likely trigger this event from time to time due to need to make changes or login to multiple devices in an environment in a short time. So verify if this is the case before escalation.

Detection Algorithm

Spike in Number of Occurrences

Criteria to Filter Event

baseeventid EQUAL TO 4624 [or]
baseeventid EQUAL TO 528 [or]
baseeventid EQUAL TO 540
AND
customnumber 1 contains 10.0
AND
Account Name NOT EQUAL TO - [and]
Account Name DOES NOT CONTAIN $ [and]
Account Name DOES NOT CONTAIN LOCAL [and]
Account Name DOES NOT CONTAIN ANONYMOUS
AND
IPAddress NOT EQUAL TO 0.0.0.0 [and]
IPAddress NOT EQUAL TO -

Verbose Info

Account: ${accountname!"ACCOUNTNAME"} IP address: ${ipaddress!"UNKNOWN"} Host: ${resourcename!"UNKNOWN"} Destination User: ${destinationusername!"UNKNOWN"} Message: ${message!"UNKNOWN"} EventID: ${baseeventid!"UNKNOWN"}

Response Bot Fields/Attributes/Policies

doneAbnormal number of remote logon attempts-SIEM-13
Abnormal number of remote logon attempts

Detection of Possible Backdoor

Criticality: Low
Applies to: Functionality
Policy Category: Malware

Device Category
Windows

Description
Possible backdoor detected in the system. Backdoor is a sign of system compromise.

Analytical Type
Real Time Policy

Prerequisites
- windows logs
- IP Attribution

Violation Entity
Resource Group Account

Threat Focus Area
Cyber

Threat Indicator
Possible backdoor account

Kill Chain Stage
Exploit

Remediation Steps
Nessus LaunchScan; NessusConnector StopScan; NessusConnector FetchScan; AD BlockUser; AD UnBlockUser; Tanium - Machine Information; Tanium - Running Processes with MD5; Tanium - Running Applications; Tanium - Non-Approved Established Connections; Tanium - User Sessions

Detection Algorithm
Individual Event Analytics

Criteria to Filter Event
Event ID EQUAL TO 4688 [or] Event ID EQUAL TO 4697
AND
Source Process Name CONTAINS Derusbi [or] Source Process Name CONTAINS winnti [or] Source Process Name CONTAINS Pirpi [or] Source Process Name CONTAINS Netbus [or] Source Process Name CONTAINS NetTraveler [or] Source Process Name CONTAINS dropper [or] Source Process Name CONTAINS Zurgop.BK [or] Source Process Name CONTAINS Brantall [or] Source Process Name CONTAINS Prardrukat [or] Source Process Name CONTAINS Small.fz [or] Source Process Name CONTAINS VBS.agent.cm [or] Source Process Name CONTAINS PlugX [or] Source Process Name CONTAINS 9002 RAT [or] requestclientapplication CONTAINS Derusbi [or] requestclientapplication CONTAINS winnti [or] requestclientapplication EQUAL TO Pirpi [or] requestclientapplication CONTAINS Netbus [or] requestclientapplication CONTAINS NetTraveler [or] requestclientapplication CONTAINS dropper [or] requestclientapplication CONTAINS Zurgop.BK [or] requestclientapplication CONTAINS Brantall [or] Source Process Name CONTAINS Prardrukat [or] requestclientapplication CONTAINS Small.fz [or] requestclientapplication CONTAINS VBS.agent.cm [or] requestclientapplication CONTAINS PlugX [or] requestclientapplication CONTAINS 9002 RAT
AND
Account Name NOT EQUAL TO - [and]
Account Name DOES NOT CONTAIN LOCAL [and]
Account Name DOES NOT CONTAIN ANONYMOUS [and]

Account Name DOES NOT CONTAIN $

Verbose Info
Account: ${accountname!"ACCOUNTNAME"} IP address: ${ipaddress!"UNKNOWN"} Host: ${resourcename!"UNKNOWN"} Destination User: ${destinationusername!"UNKNOWN"} Message: ${message!"UNKNOWN"} EventID: ${baseeventid!"UNKNOWN"}

Response Bot Fields/Attributes/Policies
Rare process creation on an endpoint
Suspicious Service creation
Rare token elevation for process
Rare process spawned by a parent process

High Number of Accounts from the Same IP Address for Successful Authentications or Run as Events
Criticality: Low
Applies to: Functionality
Policy Category: Malware

Device Category
Windows

Description
Detects high number of successful authentication events from the same ipaddress that could indicate successful lateral movement in an environment.

Analytical Type
Tier 2 Behavior Summary

Prerequisites
- windows logs
- Behavior profiles

Violation Entity
Resource Group Account

Threat Focus Area
Cyber

Threat Indicator
High number of accounts from the same ipaddress for authentication failures or lockout events

Kill Chain Stage
Recon

Remediation Steps

- VirusTotal ScanIP
- Nessus LaunchScan
- NessusConnector StopScan
- NessusConnector FetchScan
- AD BlockUser
- AD UnBlockUser
- Tanium - Machine Information
- Tanium - Running Processes with MD5
- Tanium - Running Applciations
- Tanium - Non-approved Established Connections

Detection Algorithm
Enumeration Behavior

Criteria to Filter Event
baseeventid EQUAL TO 4625 [or]
baseeventid EQUAL TO 4740 [or]
baseeventid EQUAL TO 4771

Verbose Info
Account: ${accountname!"ACCOUNTNAME"} IP address: ${ipaddress!"UNKNOWN"} Host: ${resourcename!"UNKNOWN"} Destination User: ${destinationusername!"UNKNOWN"} Message: ${message!"UNKNOWN"} EventID: ${baseeventid!"UNKNOWN"}

Response Bot Fields/Attributes/Policies
Suspicious Account Activity - Peak Explicit Credentials Distinct Account Name For Host Analytic
Abnormal number of failed logons from an ipaddress-SIEM-13
Abnormal number of logon failures-SIEM-13
Abnormal number of remote logon attempts-SIEM-13
Abnormal number of logon failures from an account-SIEM-13
Abnormal number of failed logons on a resource- SIEM-13
Multiple failed logons
Abnormal number of logon failures
Suspicious Logon Attempts
Abnormal number of remote logon attempt
Rare host accessed by an account - Logon Failure
Abnormal number of remote logon attempts
Abnormal number of failed logons on a resource- SIEM-17
Abnormal number of failed logons from an ipaddress-SIEM-17

High Number of Accounts Used on a Workstation for Successful Authentications or Run as Events
Criticality: Low
Applies to: Functionality
Policy Category: Malware

Device Category
Windows

Description
Detects high number of successful authentication or run-as events on a workstation that could indicate successful lateral movement in an environment.

Analytical Type
Tier 2 Behavior Summary

Prerequisites
- windows logs
- Behavior profiles

Violation Entity
Resources

Threat Focus Area
Cyber

Threat Indicator
High number of accounts used on a workstation for successful authentications or run as events

Kill Chain Stage
Recon

Remediation Steps
- VirusTotal ScanIP
- Nessus LaunchScan
- NessusConnector StopScan
- NessusConnector FetchScan
- AD BlockUser
- AD UnBlockUser
- Tanium - Machine Information
- Tanium - Running Processes with MD5
- Tanium - Running Applciations
- Tanium - Non-approved Established Connections

Detection Algorithm
Enumeration Behavior

Criteria to Filter Event
baseeventid EQUAL TO 4624 [and]
CustomNumber 1 EQUAL TO 10.0
OR
baseeventid EQUAL TO 4648
AND
Account Name NOT EQUAL TO - [and]
Account Name DOES NOT CONTAIN LOCAL [and]
Account Name DOES NOT CONTAIN ANONYMOUS [and]
Account Name DOES NOT CONTAIN $

Verbose Info
Account: ${accountname!"ACCOUNTNAME"} IP address: ${ipaddress!"UNKNOWN"} Host: ${resourcename!"UNKNOWN"} Destination User: ${destinationusername!"UNKNOWN"} Message: ${message!"UNKNOWN"} EventID: ${baseeventid!"UNKNOWN"}

Response Bot Fields/Attributes/Policies

Abnormal number of failed logons from an ipaddress-SIEM-13
Abnormal number of logon failures-SIEM-13
Abnormal number of remote logon attempts-SIEM-13
Abnormal number of failed logons on a resource- SIEM-13
Multiple failed logons
Abnormal number of logon failures
Suspicious Logon Attempts
Abnormal number of remote logon attempt
Abnormal number of remote logon attempts
Abnormal number of failed logons from an ipaddress-SIEM-17
Abnormal number of failed logons on a resource- SIEM-17
High number of accounts from the same ipaddress for successful authentications or run as events
High number of accounts from the same ipaddress for authentication failures or lockout events

Password Hash Access

Criticality: Low
Applies to: Functionality
Policy Category: Malware

Device Category

Windows

Description

The password hash access event may be indicative of an attempt to take over the account whose password hash was accessed.

Technique Used

Entity attribution

Analytical Type

Real Time Policy

Prerequisites

- windows logs

Violation Entity

Activity Account

Threat Focus Area

Cyber

Threat Indicator

Password hash access

Kill Chain Stage

Recon

Remediation Steps

Possible steps for further analysis / triage to consider:

1. Determine if the account has other anomalies.
2. Determine if the account should be performing the activity via a role to privilege comparison.
3. Determine if the endpoint has other anomalies associated with its processes, sessions, or network connections.

Possible Remediation steps after further analysis and triage:

1. Submit a ticket to disable the source account.
2. Submit a ticket to reset the password of the account whose hash was accessed.
3. Submit a ticket to scan host for vulnerabilities & malware (As Needed)
4. Open an investigation as per internal IR playbook dictates.

Detection Algorithm

Individual event analytics

Criteria to Filter Event

baseeventid EQUAL TO 686 [or]
baseeventid EQUAL TO 4782
AND
Account Name NOT EQUAL TO - [and]
Account Name DOES NOT CONTAIN $ [and]
Account Name DOES NOT CONTAIN LOCAL [and]
Account Name DOES NOT CONTAIN ANONYMOUS
AND
u_id not equal to -1

Risk Boosters

Active List:
accountname in suspicious_host_accessed [and/or]
employeeid in:
- Possible_bruteforce
- suspicious_process_anomaly
- suspicious_AD_authentication
- possible_privilege_misuse
- vulnerable_endpoints
- infected_endpoints
increase factor 4.0

Verbose Info

Account: ${accountname!"ACCOUNTNAME"} IP address: ${ipaddress!"UNKNOWN"} Host: ${resourcename!"UNKNOWN"} Destination User: ${destinationusername!"UNKNOWN"} Message: ${message!"UNKNOWN"} EventID: ${baseeventid!"UNKNOWN"}

Response Bot Fields/Attributes/Policies

Pass the hash detection - Key length analysis
Pass the hash detection - Randomly generated hosts
Suspicious Process Activity - Endpoint - Potential Mimikatz Object Handling Activity Analytic
Suspicious Process Activity - Potential Mimikatz or Hash Passing Token Creation - Powershell Privileged Service Call Analytic
Suspicious Account Activity - Potential pass-the-hash - Host Length Analytic
Suspicious Account Activity - Potential pass-the-hash - Key Length Analytic
Use of credential dumpers
Rare process creation on an endpoint
Suspicious Service creation
Rare service created on endpoint

Rare process spawned by a parent process
Rare process detected for authentication using explicit credentials

Possible AD Enumeration

Criticality: Medium
Applies to: Functionality
Policy Category: Malware

Device Category

Windows

Description

This may be indicative of a possible LDAP scanning event caused by a malicious presence. Enumeration of privileges is typically leveraged by malwares to achieve privilege escalation.

Technique Used

Entity attribution

Analytical Type

Real Time Policy

Prerequisites

- windows logs

Violation Entity

Activity Account

Threat Focus Area

Cyber

Threat Indicator

Possible privilege enumeration

Kill Chain Stage

Exploit

Remediation Steps

- Nessus LaunchScan
- NessusConnector StopScan
- NessusConnector FetchScan
- AD BlockUser
- AD UnBlockUser
- Tanium - Machine Information
- Tanium - Running Processes with MD5
- Tanium - Running Applciations
- Tanium - Non-approved Established Connections

Detection Algorithm

Individual event analytics

Criteria to Filter Event

baseeventid EQUAL TO 4798 [or]
baseeventid EQUAL TO 4799
AND
Account Name DOES NOT CONTAIN $ [and]
Account Name DOES NOT CONTAIN LOCAL [and]
Account Name DOES NOT CONTAIN ANONYMOUS

Risk Boosters

Active List:
employeeid in Suspicious_ad_authentication increase factor 4.0

Verbose Info

Account: ${accountname!"ACCOUNTNAME"} IP address: ${ipaddress!"UNKNOWN"} Host: ${resourcename!"UNKNOWN"} Message: ${message!"UNKNOWN"} EventID: ${baseeventid!"UNKNOWN"}

Response Bot Fields/Attributes/Policies

Abnormal number of privileges enumerated
Abnormal number of accounts enumerated
Rare account enumeration event
Rare privilege enumeration event
Abnormal number of account enumeration attempts on an endpoint
Possible Privilege Enumeration
Suspicious AD Enumeration Observed

Possible Impersonation Detected

Criticality: Low
Applies to: Functionality
Policy Category: Malware

Device Category

Windows

Description

Detects events that may indicate an attacker is collecting Kerberos Service Tickets for decryption to impersonate the embedded service accounts.

Analytical Type

Directive Based

Prerequisites

- windows logs

Violation Entity

Resource Group Account

Threat Focus Area

Cyber

Threat Indicator

Possible account enumeration

Kill Chain Stage
Exploit

Remediation Steps
- Nessus LaunchScan
- NessusConnector StopScan
- NessusConnector FetchScan
- AD BlockUser
- AD UnBlockUser
- Tanium - Machine Information
- Tanium - Running Processes with MD5
- Tanium - Running Applciations
- Tanium - Non-approved Established Connections

Criteria to Filter Event
Account Name DOES NOT CONTAIN filepath [and]
baseeventid EQUAL TO 4769 [and]
filepath NOT EQUAL TO krbtgt [and]
Account Name DOES NOT CONTAIN $ [and]
filepath DOES NOT CONTAIN LDAP

Additional Event Analytics
Detects when an account access 5 different network services in a 10 minute time period

Directives
Name MultipleTickets
Filter for Events matching criteria? NA
Having similar accountname
Number of Occurrences 5
Within Duration 00:10:00
Should events happen consecutively? false
Distinct? filepath

Verbose Info
Account ${accountname!"ACCOUNTNAME"} performed ${transactionstring1!"ACTIVITY"} from ipaddress ${ipaddress!"UNKNOWN"}

Response Bot Fields/Attributes/Policies
Abnormal number of Kerberos impersonation attempts detected -13
Abnormal object or network share access attempts by resource-SIEM-13
Abnormal object or network share access attempts-SIEM-13
Abnormal number of service tickets requested-SIEM-13
Abnormal number of network share object access
Unusual high number of network shares accessed - SIEM
Suspicious Account Activity - Kerberoasting - Peak TGS Request For User Analytic
Suspicious Account Activity - Kerberoasting - Rare TGS Encryption Type For User Analytic
Suspicious Process Activity - Endpoint - Potential Mimikatz Object Handling Activity Analytic
Use of credential dumpers
Abnormal number of hosts accessed-SIEM-13
Abnormal number of hosts accessed
Suspicious host access behavior from an account

Possible Privilege Enumeration

Criticality: Medium
Applies to: Functionality
Policy Category: Malware

Device Category

Windows

Description

This may be indicative of a possible LDAP scanning event caused by a malicious presence. Enumeration of privileges is typically leveraged by malwares to achieve privilege escalation.

Technique Used

Entity Attribution

Analytical Type

Real Time Policy

Prerequisites

- windows logs

Violation Entity

Activity Account

Threat Focus Area

Cyber

Threat Indicator

Possible privilege enumeration

Kill Chain Stage

Exploit

Remediation Steps

- Nessus LaunchScan
- NessusConnector StopScan
- NessusConnector FetchScan
- AD BlockUser
- AD UnBlockUser
- Tanium - Machine Information
- Tanium - Running Processes with MD5
- Tanium - Running Applciations
- Tanium - Non-approved Established Connections

Detection Algorithm

Individual event analytics

Criteria to Filter Event

baseeventid EQUAL TO 4798 [or]
baseeventid EQUAL TO 4799

AND
Account Name DOES NOT CONTAIN $ [and]
Account Name DOES NOT CONTAIN LOCAL [and]
Account Name DOES NOT CONTAIN ANONYMOUS
Account Name NOT EQUAL TO -

Risk Boosters
Active list:
employeeid in possible_privilege_misuse increase factor 4.0

Verbose Info
Account: ${accountname!"ACCOUNTNAME"} IP address: ${ipaddress!"UNKNOWN"} Host: ${resourcename!"UNKNOWN"} Destination User: ${destinationusername!"UNKNOWN"} Message: ${message!"UNKNOWN"} EventID: ${baseeventid!"UNKNOWN"}

Response Bot Fields/Attributes/Policies
Abnormal number of privileges enumerated
Rare privilege enumeration event
Possible AD Enumeration
Abnormal number of accounts enumerated
Rare account enumeration event
Suspicious AD Enumeration Observed

Rare Basic Service Operation
Criticality: Low
Applies to: Functionality
Policy Category: Malware

Device Category
Windows

Description
Detects basic service operations that haven't been seen before.

Analytical Type
Tier 2 Behavior Summary

Prerequisites
- windows logs
- Behavior profiles

Violation Entity
Resource Group Account

Threat Focus Area
Cyber

Threat Indicator
Rare basic service operation

Kill Chain Stage
Recon

Remediation Steps
- AD BlockUser
- AD UnBlockUser
- Tanium - Machine Information
- Tanium - Running Processes with MD5
- Tanium - Running Applciations
- Tanium - Non-approved Established Connections

Detection Algorithm
Rare behavior

Criteria to Filter Event
baseeventid EQUAL TO 7036
AND
Account Name DOES NOT CONTAIN $ [and]
Account Name DOES NOT CONTAIN LOCAL [and]
Account Name DOES NOT CONTAIN ANONYMOUS [and]
Account Name NOT EQUAL TO -

Verbose Info
Account: ${accountname!"ACCOUNTNAME"} IP address: ${ipaddress!"UNKNOWN"} Host: ${resourcename!"UNKNOWN"} Destination User: ${destinationusername!"UNKNOWN"} Message: ${message!"UNKNOWN"} EventID: ${baseeventid!"UNKNOWN"}

Response Bot Fields/Attributes/Policies
Certificate Service Status
Rare process creation on an endpoint
Rare token elevation for process
Rare process spawned by a parent process
Rare process detected for authentication using explicit credentials
Suspicious Process Activity - Log Clearing Analytics
Suspicious Process Activity - Potential Mimikatz or Hash Passing Token Creation - Powershell Privileged Service Call Analytic
Suspicious Process Activity - Endpoint - Potential Mimikatz Object Handling Activity Analytic
Detection of possible backdoor
Use of credential dumpers
Rare service created on endpoint
Suspicious Service creation

Rare Logon Process Detected for Windows Authentication
Criticality: None
Applies to: Functionality
Policy Category: Malware

Device Category
Windows

Description
Rare logon process for an account indicates a change in the typical authentication pattern for an account. This could indicate an account being misused or using unauthorized elevated privileges.

Technique Used
Behavior anomaly for rarity on logon process

Analytical Type
Tier 2 Behavior Summary

Prerequisites
- windows logs
- Behavior profiles

Violation Entity
Resource Group Account

Threat Focus Area
Cyber

Threat Indicator
Suspicious Process execution

Kill Chain Stage
Execute

Remediation Steps
- Nessus LaunchScan
- NessusConnector StopScan
- NessusConnector FetchScan
- AD BlockUser
- AD UnBlockUser
- Tanium - Machine Information
- Tanium - Running Processes with MD5
- Tanium - Running Applciations
- Tanium - Non-approved Established Connections

Detection Algorithm
Rare behavior

Criteria to Filter Event
baseeventid EQUAL TO 528 [or]
baseeventid EQUAL TO 540 [or]
baseeventid EQUAL TO 4624
AND
Account Name DOES NOT CONTAIN $ [and]
Account Name DOES NOT CONTAIN LOCAL [and]
Account Name DOES NOT CONTAIN ANONYMOUS [and]
Account Name NOT EQUAL TO -

Verbose Info
Account: ${accountname!"ACCOUNTNAME"} IP address: ${ipaddress!"UNKNOWN"} Host: ${resourcename!"UNKNOWN"} Destination User: ${destinationusername!"UNKNOWN"} Message: ${message!"UNKNOWN"} EventID: ${baseeventid!"UNKNOWN"}

Response Bot Fields/Attributes/Policies

Rare host accessed by an account - Logon Success
Rare host accessed by an account - Logon Failure
Rare logon type detected for an account
Rare object access attempts by an account
Firewall disabled on windows
Rare audit log clearing by an account
Rare registry modification by an account
Rare regedit usage compared to peer
Rare process creation on an endpoint
Abnormal number of process execution using explicit credentials
Rare Basic Service Operation
Rare token elevation for process
Detection of possible backdoor
Use of credential dumpers
Rare process detected for authentication using explicit credentials
Suspicious Registry Modification Observed
Suspicious Process Activity - Log Clearing Analytics
Suspicious Process Activity - Potential Mimikatz or Hash Passing Token Creation - Powershell Privileged Service Call Analytic
Suspicious Process Activity - Endpoint - Potential Mimikatz Object Handling Activity Analytic

Rare Logon Type Detected for an Account

Criticality: None
Applies to: Functionality
Policy Category: Malware

Device Category

Windows

Description

Rare logon type for an account indicates a change in the typical authentication pattern for an account. This could indicate an account being misused or using unauthorized elevated privileges

Technique Used

Behavior anomaly for rarity on logon type

Analytical Type

Tier 2 Behavior Summary

Prerequisites

- windows logs
- Behavior profiles

Violation Entity

Resource Group Account

Threat Focus Area

Cyber

Threat Indicator

Suspicious AD Authentication

Kill Chain Stage

Recon

Remediation Steps
- AD BlockUser
- AD UnBlockUser
- Tanium - Machine Information
- Tanium - Running Processes with MD5
- Tanium - Running Applciations
- Tanium - Non-approved Established Connections

Detection Algorithm
Rare behavior

Criteria to Filter Event
baseeventid EQUAL TO 4624 [or]
baseeventid EQUAL TO 528 [or]
baseeventid EQUAL TO 540
AND
Account Name NOT EQUAL TO NA [and]
Account Name NOT EQUAL TO - [and]
Account Name DOES NOT CONTAIN $ [and]
Account Name DOES NOT CONTAIN LOCAL [and]
Account Name DOES NOT CONTAIN ANONYMOUS

Verbose Info
Account: ${accountname!"ACCOUNTNAME"} IP address: ${ipaddress!"UNKNOWN"} Host: ${resourcename!"UNKNOWN"} Message: ${message!"UNKNOWN"} EventID: ${baseeventid!"UNKNOWN"}

Response Bot Fields/Attributes/Policies
Use of explicit credentials - Account sharing or Password misuse
New admin account detected
Rare target account authentication using explicit credentials
Rare logon process detected for windows authentication

Rare Privileged Level for Windows Authentication
Criticality: None
Applies to: Functionality
Policy Category: Malware

Device Category
Windows

Description
Rare privilege level for a new logon indicates a change in the typical authentication pattern for an account. This could indicate an account being misused or using unauthorized elevated privileges.

Technique Used
Behavior anomaly for rarity on privilege level

Analytical Type
Tier 2 Behavior Summary

Prerequisites
- windows logs
- Behavior profiles

Violation Entity
Activity Account

Threat Focus Area
Cyber

Threat Indicator
Possible privilege misuse

Kill Chain Stage
Delivery

Remediation Steps
- AD BlockUser
- AD BlockUser
- AD UnBlockUser
- Tanium - Machine Information
- Tanium - Running Processes with MD5
- Tanium - Running Applciations
- Tanium - Non-approved Established Connections

Detection Algorithm
Rare behavior

Criteria to Filter Event
baseeventid EQUAL TO 4672
AND
Account Name DOES NOT CONTAIN LOCAL [and]
Account Name DOES NOT CONTAIN ANONYMOUS [and]
Account Name NOT EQUAL TO - [and]
Account Name DOES NOT CONTAIN $

Verbose Info
Account: ${accountname!"ACCOUNTNAME"} IP address: ${ipaddress!"UNKNOWN"} Host: ${resourcename!"UNKNOWN"} Destination User: ${destinationusername!"UNKNOWN"} Message: ${message!"UNKNOWN"} EventID: ${baseeventid!"UNKNOWN"}

Response Bot Fields/Attributes/Policies
Possible Privilege Escalation - Self Escalation
Abnormal number of privileges enumerated
Rare privileged events performed by user compared to peer
Rare privilege enumeration event
Possible Privilege Enumeration
Suspicious Process Activity - Potential Mimikatz or Hash Passing Token Creation - Powershell Privileged Service Call Analytic
Possible AD Enumeration
Abnormal number of account enumeration attempts on an endpoint
Suspicious AD Enumeration Observed

Rare Process Creation on an Endpoint

Criticality: None
Applies to: Functionality
Policy Category: Malware

Device Category

Windows

Description

This anomaly may be indicative of a possible malicious process being executed, additional indicators like path of execution would determine the severity.

Technique Used

Behavior anomaly on process execution on an endpoint

Analytical Type

Tier 2 Behavior Summary

Prerequisites

- windows logs
- Behavior profiles

Violation Entity

Resource Group Account

Threat Focus Area

Cyber

Threat Indicator

Suspicious Process execution

Kill Chain Stage

Execute

Remediation Steps

- Nessus LaunchScan
- NessusConnector StopScan
- NessusConnector FetchScan
- AD BlockUser
- AD UnBlockUser
- Tanium - Machine Information
- Tanium - Running Processes with MD5
- Tanium - Running Applciations
- Tanium - Non-approved Established Connections

Detection Algorithm

Rare behavior

Criteria to Filter Event

[or][and]
baseeventid EQUAL TO 4688
AND
Account Name DOES NOT CONTAIN ANONYMOUS [and]

Account Name NOT EQUAL TO - [and]
Account Name DOES NOT CONTAIN LOCAL [and]
Account Name DOES NOT CONTAIN $ [and]

Verbose Info
Account: ${accountname!"ACCOUNTNAME"} IP address: ${ipaddress!"UNKNOWN"} Host: ${resourcename!"UNKNOWN"} Destination User: ${destinationusername!"UNKNOWN"} Message: ${message!"UNKNOWN"} EventID: ${baseeventid!"UNKNOWN"}

Response Bot Fields/Attributes/Policies
Suspicious Service creation
Rare service created on endpoint
Rare token elevation for process
Rare Basic Service Operation
Use of credential dumpers
Detection of possible backdoor
Rare process spawned by a parent process
Rare logon process detected for windows authentication
Rare process detected for authentication using explicit credentials
Suspicious Process Activity - Log Clearing Analytics
Suspicious Process Activity - Potential Mimikatz or Hash Passing Token Creation - Powershell Privileged Service Call Analytic
Suspicious Process Activity - Endpoint - Potential Mimikatz Object Handling Activity Analytic
Suspicious executables on a machine

Rare Process Detected for Authentication Using Explicit Credentials
Criticality: None
Applies to: Functionality
Policy Category: Malware

Device Category
Windows

Description
Rare process for authentication using explicit credentials could indicate an authentication with elevated privileges. This type of activity coupled with other authentication anomalies could indicate lateral propagation

Technique Used
Behavior anomaly for rarity on process

Analytical Type
Tier 2 Behavior Summary

Prerequisites
- windows logs
- Behavior profiles

Violation Entity
Activity Account

Threat Focus Area
Cyber

Threat Indicator
Suspicious Process execution

Kill Chain Stage
Execute

Remediation Steps
- Nessus LaunchScan
- NessusConnector StopScan
- NessusConnector FetchScan
- AD BlockUser
- AD UnBlockUser
- Tanium - Machine Information
- Tanium - Running Processes with MD5
- Tanium - Running Applciations
- Tanium - Non-approved Established Connections

Detection Algorithm
Rare behavior

Criteria to Filter Event
baseeventid EQUAL TO 4648
AND
oldfilepath CONTAINS C:\Windows\System32 [and]
Source Process Name DOES NOT CONTAIN lsass.exe [and]
Source Process Name DOES NOT CONTAIN winlogon.exe [and]
Source Process Name DOES NOT CONTAIN svchost.exe [and]
Source Process Name DOES NOT CONTAIN services.exe
OR
oldfilepath CONTAINS C:\Program files [and]
oldfilepath DOES NOT CONTAIN SASHome [and]
oldfilepath DOES NOT CONTAIN MVPSI/JAMS/Agent [and]
oldfilepath DOES NOT CONTAIN Microsoft Office [and]
oldfilepath DOES NOT CONTAIN avs [and]
oldfilepath DOES NOT CONTAIN Internet Explorer [and]
oldfilepath DOES NOT CONTAIN Microsoft SQL Server [and]
oldfilepath DOES NOT CONTAIN Chrome
OR
oldfilepath DOES NOT CONTAIN D:\Program Files\avs [and]
oldfilepath DOES NOT CONTAIN D:\MVPSI\JAMS\
AND
Account Name NOT EQUAL TO - [and]
Account Name DOES NOT CONTAIN $ [and]
Account Name DOES NOT CONTAIN ANONYMOUS [and]
Account Name DOES NOT CONTAIN LOCAL

Verbose Info

Account: ${accountname!"ACCOUNTNAME"} IP address: ${ipaddress!"UNKNOWN"} Host: ${resourcename!"UNKNOWN"} Destination User: ${destinationusername!"UNKNOWN"} Message: ${message!"UNKNOWN"} EventID: ${baseeventid!"UNKNOWN"}

Response Bot Fields/Attributes/Policies

Rare process creation on an endpoint
Suspicious Service creation
Rare service created on endpoint
Abnormal number of process execution using explicit credentials
Rare Basic Service Operation
Rare token elevation for process
Use of credential dumpers
Detection of possible backdoor
Rare process spawned by a parent process
Rare logon process detected for windows authentication
Suspicious Process Activity - Log Clearing Analytics
Suspicious Process Activity - Potential Mimikatz or Hash Passing Token Creation - Powershell Privileged Service Call Analytic
Suspicious Process Activity - Endpoint - Potential Mimikatz Object Handling Activity Analytic
Suspicious executables on a machine

Rare Process Spawned by a Parent Process

Criticality: None
Applies to: Functionality
Policy Category: Malware

Device Category

Windows

Description

This anomaly may be indicative of a possible malicious process being executed, additional indicators like path of execution would determine the severity.

Technique Used

Behavior anomaly on process execution on an endpoint

Analytical Type

Tier 2 Behavior Summary

Prerequisites

- windows logs
- Behavior profiles

Violation Entity

Activity Account

Threat Focus Area

Cyber

Threat Indicator

Suspicious Process execution

Kill Chain Stage

Execute

Remediation Steps

- Nessus LaunchScan
- NessusConnector StopScan
- NessusConnector FetchScan
- AD BlockUser
- AD UnBlockUser
- Tanium - Machine Information
- Tanium - Running Processes with MD5
- Tanium - Running Applciations
- Tanium - Non-approved Established Connections

Detection Algorithm

Rare behavior

Criteria to Filter Event

baseeventid EQUAL TO 592 [or]
baseeventid EQUAL TO 4688
AND
Account Name DOES NOT CONTAIN $ [and]
Account Name DOES NOT CONTAIN LOCAL [and]
Account Name DOES NOT CONTAIN ANONYMOUS [and]
Account Name NOT EQUAL TO -

Additional Event Analytics

Match Criteria:
oldfilepath contains C:\Windows\Fonts\ [or]
oldfilepath contains C:\users\ [or]
oldfilepath contains C:\windows\help [or]
oldfilepath contains C:\windows\wbem [or]
oldfilepath contains C:\windows\addins [or]
oldfilepath contains C:\windows\debut [or]
oldfilepath contains C:\windows\system32\tasks [or]
oldfilepath contains C:\Users\%Temp%
increase factor 0.3

Verbose Info

Account: ${accountname!"ACCOUNTNAME"} IP address: ${ipaddress!"UNKNOWN"} Host: ${resourcename!"UNKNOWN"} Destination User: ${destinationusername!"UNKNOWN"} Message: ${message!"UNKNOWN"} EventID: ${baseeventid!"UNKNOWN"}

Response Bot Fields/Attributes/Policies

Rare process creation on an endpoint
Rare token elevation for process
Rare Basic Service Operation
Detection of possible backdoor
Rare process detected for authentication using explicit credentials
Suspicious Process Activity - Log Clearing Analytics
Suspicious Process Activity - Potential Mimikatz or Hash Passing Token Creation - Powershell Privileged Service Call Analytic
Suspicious Process Activity - Endpoint - Potential Mimikatz Object Handling Activity Analytic
Suspicious executables on a machine

Rare Token Elevation for Process

Criticality: None

Applies to: Functionality
Policy Category: Malware

Device Category
Windows

Description
Rare token elevation for a process could indicate a process created with elevated privileges. This process can be used by a malicious actor to exploit a vulnerability

Technique Used
Behavior anomaly for rarity on token elevation

Analytical Type
Tier 2 Behavior Summary

Prerequisites
- windows logs
- Behavior profiles

Violation Entity
Activity Account

Threat Focus Area
Cyber

Threat Indicator
Suspicious Process execution

Kill Chain Stage
Execute

Remediation Steps
- Nessus LaunchScan
- NessusConnector StopScan
- NessusConnector FetchScan
- AD BlockUser
- AD UnBlockUser
- Tanium - Machine Information
- Tanium - Running Processes with MD5
- Tanium - Running Applciations
- Tanium - Non-approved Established Connections

Detection Algorithm
Rare behavior

Criteria to Filter Event
baseeventid EQUAL TO 4688
AND
Account Name DOES NOT CONTAIN $ [and]
Account Name DOES NOT CONTAIN LOCAL [and]
Account Name DOES NOT CONTAIN ANONYMOUS [and]

Account Name NOT EQUAL TO -

Verbose Info
Account: ${accountname!"ACCOUNTNAME"} IP address: ${ipaddress!"UNKNOWN"} Host: ${resourcename!"UNKNOWN"} Destination User: ${destinationusername!"UNKNOWN"} Message: ${message!"UNKNOWN"} EventID: ${baseeventid!"UNKNOWN"

Response Bot Fields/Attributes/Policies
Rare token elevation for process

Replay Attack Detection
Criticality: Low
Applies to: Functionality
Policy Category: Malware

Device Category
Windows

Description
A replay attack occurs when an intruder steals a packet from the network and forwards that packet to a service or application as if the intruder was the user who originally sent the packet. When the packet is an authentication packet, the intruder can use the replay attack to authenticate on another person's behalf and consequently access that person's resources or data.

Technique Used
Entity Attribution

Analytical Type
Tier 2 Behavior Summary

Prerequisites
- windows logs

Violation Entity
Activity Account

Threat Focus Area
Cyber

Threat Indicator
Replay attack detection

Kill Chain Stage
Execute

Remediation Steps
- Nessus LaunchScan
- NessusConnector StopScan
- NessusConnector FetchScan
- AD BlockUser
- AD UnBlockUser

- Tanium - Machine Information
- Tanium - Running Processes with MD5
- Tanium - Running Applciations
- Tanium - Non-approved Established Connections

Detection Algorithm
Individual Event Analytics

Criteria to Filter Event
baseeventid EQUAL TO 4649
AND
Account Name NOT EQUAL TO - [and]
Account Name DOES NOT CONTAIN $ [and]
Account Name DOES NOT CONTAIN LOCAL [and]
Account Name DOES NOT CONTAIN ANONYMOUS

Risk Boosters
Active List:
accountname in suspicious_host_accessed [and/or]
employeeid in:
- Possible_bruteforce
- suspicious_process_anomaly
- suspicious_AD_authentication
- possible_privilege_misuse
- vulnerable_endpoints
- infected_endpoints
increase factor 4.0

Verbose Info
Account: ${accountname!"ACCOUNTNAME"} IP address: ${ipaddress!"UNKNOWN"} Host: ${resourcename!"UNKNOWN"} Destination User: ${destinationusername!"UNKNOWN"} Message: ${message!"UNKNOWN"} EventID: ${baseeventid!"UNKNOWN"}

Response Bot Fields/Attributes/Policies
Abnormal number of successful authentication attempts
Rare logon type detected for an account
- Hard to choose for this as the replay should in theory be successful.

Spike in Administrative Shares Accessed
Criticality: Medium
Applies to: Functionality
Policy Category: Malware

Device Category
Windows

Description
A spike in account accessing administrative share objects may be indicative of recon activity to exploit an endpoint

Technique Used
Behavior anomaly on administrative share access activity

Analytical Type
Tier 2 Behavior Summary

Prerequisites
- windows logs
- Behavior profiles

Violation Entity
Resource Group Account

Threat Focus Area
Cyber

Threat Indicator
Suspicious Network Share Access

Kill Chain Stage
Recon

Remediation Steps
- Nessus LaunchScan
- NessusConnector StopScan
- NessusConnector FetchScan
- AD BlockUser
- AD UnBlockUser
- Tanium - Machine Information
- Tanium - Running Processes with MD5
- Tanium - Running Applciations
- Tanium - Non-approved Established Connections

Detection Algorithm
Spike in number of occurrences

Criteria to Filter Event
baseeventid EQUAL TO 5145 [or]
baseeventid EQUAL TO 5140
AND
Resource CustomField 5 CONTAINS $ [and]
Resource CustomField 5 CONTAINS $ [and]
Account Name DOES NOT CONTAIN $ [and]
Account Name DOES NOT CONTAIN ANONYMOUS
AND
Account Name DOES NOT CONTAIN LOCAL [and]
Account Name NOT EQUAL TO -

Risk Boosters
Match criteria:
resource customfield 5 starts with ADMIN increase factor 5.0

Verbose Info
Account: ${accountname!"ACCOUNTNAME"} IP address: ${ipaddress!"UNKNOWN"} Host: ${resourcename$LIST!"UNKNOWN"} Share Name: ${resourcecustomfield5$LIST!"UNKNOWN"} Message: ${message!"UNKNOWN"} EventID: ${baseeventid!"UNKNOWN"}

Response Bot Fields/Attributes/Policies
Abnormal object or network share access attempts by resource-SIEM-13

Abnormal number of administrative share object accessed-SIEM-13
Abnormal object or network share access attempts-SIEM-13
Rare admin share access by an account
Abnormal number of network share object access
Abnormal number of host access attempts
Abnormal number of hosts accessed
Abnormal number of administrative share object accessed
Rare host accessed by an account - Logon Failure
Rare Host Accessed Attempt By Account
Unusual high number of network shares accessed - SIEM
Rare Host Accessed from an Account
Suspicious host access behavior from an account
Rare object access attempts by an account

Unusual Service Authentication Detected for User

Criticality: None
Applies to: Functionality
Policy Category: Malware

Device Category

Windows

Description

Rare logon type for an account indicates a change in the typical authentication pattern for an account. This could indicate an account being misused or using unauthorized elevated privileges

Technique Used

Behavior anomaly for rarity on logon type

Analytical Type

Tier 2 Behavior Summary

Prerequisites

- windows logs
- Behavior profiles

Violation Entity

Resource Group Account

Threat Focus Area

Cyber

Threat Indicator

Suspicious AD Authentication

Kill Chain Stage

Recon

Remediation Steps

- AD BlockUser
- AD UnBlockUser
- Tanium - Machine Information
- Tanium - Running Processes with MD5
- Tanium - Running Applciations
- Tanium - Non-approved Established Connections

Detection Algorithm
Rare behavior

Criteria to Filter Event
baseeventid EQUAL TO 4624 [or]
baseeventid EQUAL TO 528 [or]
baseeventid EQUAL TO 540
AND
Account Name NOT EQUAL TO NA [and]
Account Name NOT EQUAL TO - [and]
Account Name DOES NOT CONTAIN $ [and]
Account Name DOES NOT CONTAIN LOCAL [and]
Account Name DOES NOT CONTAIN ANONYMOUS
AND
CustomNumber 1 EQUAL TO 4.0 [and]
CustomNumber 1 EQUAL TO 5.0
AND
u_id NOT EQUAL TO -1

Verbose Info
Account: ${accountname!"ACCOUNTNAME"} IP address: ${ipaddress!"UNKNOWN"} Host: ${resourcename!"UNKNOWN"} Message: ${message!"UNKNOWN"} EventID: ${baseeventid!"UNKNOWN"}

Response Bot Fields/Attributes/Policies
Rare Basic Service Operation
Rare logon type detected for an account

Use of Credential Dumpers
Criticality: Low
Applies to: Functionality
Policy Category: Malware

Device Category
Windows

Description
Credential dumpers usage is detected. It's used to extract credential hashes for offline cracking, extracting plaintext passwords, and extracting Kerberos tickets, among others.

Analytical Type
Real Time Policy

Prerequisites
- windows logs

Violation Entity
Resource Group Account

Threat Focus Area
Cyber

Threat Indicator
Usage of credential dumping tools

Kill Chain Stage
Exploit

Remediation Steps
- VirusTotal Scanfile
- Nessus LaunchScan
- NessusConnector StopScan
- NessusConnector FetchScan
- AD BlockUser
- AD UnBlockUser
- Tanium - Machine Information
- Tanium - Running Processes with MD5
- Tanium - Running Applciations
- Tanium - Non-approved Established Connections
- Tanium - User Sessions

Detection Algorithm
Individual event analytics

Criteria to Filter Event
Source Process Name CONTAINS WCE [or]
Source Process Name CONTAINS pwdump [or]
Source Process Name CONTAINS gsecdump [or]
Source Process Name CONTAINS Mimikatz [or]
Source Process Name CONTAINS Zhumimikatz [or]
Source Process Name CONTAINS Invoke-mimikatz [or]
Source Process Name CONTAINS QuarksPwDump [or]
Source Process Name CONTAINS hashdump [or]
Source Process Name CONTAINS GerPassword_x64 [or]
Source Process Name CONTAINS ReadPWD86 [or]
Destination Process Name CONTAINS WCE
AND
Account Name NOT EQUAL TO - [and]
Account Name DOES NOT CONTAIN LOCAL [and]
Account Name DOES NOT CONTAIN ANONYMOUS [and]
Account Name DOES NOT CONTAIN $
AND
baseeventid EQUAL TO 4688 [or]
baseeventid EQUAL TO 4657 [or]
baseeventid EQUAL TO 4663 [or]
baseeventid EQUAL TO 4624 [or]
baseeventid EQUAL TO 4625

Verbose Info

Account ${accountname!"ACCOUNTNAME"} performed ${transactionstring1!"ACTIVITY"} from ipaddress ${ipaddress!"UNKNOWN"}

Response Bot Fields/Attributes/Policies

Use of explicit credentials - Account sharing or Password misuse
Rare registry modification by an account
Rare admin share access by an account
Member added to built-in admin groups by uncorelated accounts
Rare target account authentication using explicit credentials
Suspicious Account Activity - Potential pass-the-hash - Host Length Analytic
Suspicious Account Activity - Potential pass-the-hash - Key Length Analytic
Suspicious Account Activity - Peak Credential Validation Failure Increase For Host Analytic
Suspicious Account Activity - Kerberoasting - Rare TGS Encryption Type For User Analytic
Suspicious Account Activity - Kerberoasting - Peak TGS Request For User Analytic
Suspicious Process Activity - Potential Mimikatz or Hash Passing Token Creation - Powershell Privileged Service Call Analytic
Suspicious Process Activity - Endpoint - Potential Mimikatz Object Handling Activity Analytic
Pass the hash detection - Key length analysis
Pass the hash detection - Randomly generated hosts

A Member was Added and Removed from a Security-Enabled Group within a Short Time–13

Criticality: Low
Applies to: Functionality
Policy Category: Alert

Device Category

Windows

Description

Temporarily creating and deleting an account may be indicative of a possible backdoor access attempt to use elevated privileges

Technique Used

Entity attribution

Analytical Type

Directive Based

Prerequisites

- windows logs
- Lookup Table of Support accounts / Users

Violation Entity

Resource Group Account

Threat Focus Area

Insider/Cyber

Threat Indicator

Suspicious group management event detected

Kill Chain Stage

Recon

Remediation Steps

Possible steps for further analysis / triage to consider:

1. Determine if the activity is approved by checking service management system for an incident / work order (ticket) associated with the activity.
2. Determine if the escalated account has other anomalies
3. Determine if the Source account has other anomalies.
4. Determine if the Source account or its peers have performed similar activities.
5. Determine if the account should be performing the activity via a role to privilege comparison.
6. Determine activities performed by account that was added before getting deleted

Possible Remediation steps after further analysis and triage:

1. Submit a ticket to revert any changes that occurred.
2. Submit a ticket to disable the account(s).
3. Submit a ticket to remove the account(s) (as needed)
4. Submit a ticket to revoke privileges

Detection Algorithm

Aggregated event analytics

Criteria to Filter Event

Account Name does not contain $ [and]
Account Name not equal to ANONYMOUS LOGON [and]
Account Name does not contain LOCAL [and]
Account Name not equal to -
And
baseeventid equal to 4729 [or]
baseeventid equal to 4728 [or]
baseeventid equal to 4757 [or]
baseeventid equal to 4756

Directives

Parent:
Name MemberAdded
Filter for Events matching criteria? baseeventid CONDITION_EQUALS 4728 OR baseeventid CONDITION_EQUALS 4756
Having similar accountname
Number of Occurrences 1
Within Duration 01:00:00
Should events happen consecutively? false
Distinct? NA

CHILD:
Name MemberRemoved
Filter for Events matching criteria? baseeventid CONDITION_EQUALS 4729 OR baseeventid CONDITION_EQUALS 4757
Number of Occurrences 1
Within Duration 01:00:00
Should events happen consecutively? false
Distinct? NA
Minimum duration between parent and child 12:00:00
Common between parent and child? destinationusername,devicecustomstring1

Verbose Info

Account: ${accountname!"UNKNOWN"} added and deleted User: ${destinationusername!"UNKNOWN"} from Group: ${devicecustomstring1!"UNKNOWN"} IP address: ${ipaddress!"UNKNOWN"} Message: ${message!"UNKNOWN"} EventID: ${baseeventid!"UNKNOWN"}

Response Bot Fields/Attributes/Policies

Account added and removed to security group
Possible Privilege Escalation - Self Escalation
Member added to built-in admin groups by uncorelated accounts
Rare builtin member group additions
Rare admin group member additions by user compared to peer
A member was added and removed from a security enabled group within a short time-17

Abnormal Number of Administrative Share Object Accessed

Criticality: Medium
Applies to: Functionality
Policy Category: Alert

Device Category

Windows

Description

A spike in account accessing administrative share objects may be indicative of recon activity to exploit an endpoint

Technique Used

Behavior anomaly on administrative share access activity

Analytical Type

Tier 2 Behavior Summary

Prerequisites

- Windows logs
- behavior profiles
- Server name conventions
- Service Account naming conventions

Violation Entity

Resource Group Account

Threat Focus Area

Cyber

Threat Indicator

Suspicious group management event detected

Kill Chain Stage

Recon

Remediation Steps

Possible steps for further analysis/triage to consider:

1. Determine if the activity is approved by checking service management system for an incident / work order (ticket) associated with the activity.
2. Determine if the target resources have any other anomalies.
3. Determine if the source account or its peers have performed similar activities.
4. Determine if the source account should be performing the activity via a role to privilege comparison.

5. Determine if the endpoint has other anomalies associated with its processes, sessions, or network connections.

Possible Remediation steps after further analysis and triage:

1. Submit a ticket to revert any changes that occurred.
2. Submit a ticket to disable the account.
3. Submit a ticket to remove the account (as needed)
4. Submit a ticket to revoke privileges
5. Submit a ticket to perform a full Antivirus scan
6. Submit a ticket for host isolation and further remediation as per internal IR playbooks dictate.

Detection Algorithm

Spike in Number of Occourences
Transactionstring1
Admin Share Acces-9
Transaction Occurence Abnormally higher than User's Daily Behavior
Sigma: 0.6

Criteria to Filter Event

baseeventid = 5145 [or]
baseeventid = 5140
AND
Resource CustomField 5 contains $ [and]
Account Name does not contain LOCAL [and]
Account name does not contain $ [and]
account Name does not contain ANONYMOUS

Verbose Info

Account: ${accountname!"ACCOUNTNAME"} on Host: ${resourcename!"UNKNOWN"} accessed Shares: ${resourcecustomfield5$LIST!"UNKNOWN"} Message: ${message!"UNKNOWN"} EventID: ${baseeventid!"UNKNOWN"}

Response Bot Fields/Attributes/Policies

Abnormal number of administrative share object accessed-SIEM-13
Abnormal number of network share object access
Abnormal object or network share access attempts by resource-SIEM-13
Abnormal number of hosts accessed-SIEM-13
Abnormal object or network share access attempts-SIEM-13
Rare host accessed by an account
Rare admin share access by an account
Abnormal number of host access attempts
Abnormal number of hosts accessed
Spike in administrative shares accessed
Rare host accessed by an account - Logon Failure
Rare Host Accessed Attempt By Account
Unusual high number of network shares accessed - SIEM
Rare Host Accessed from an Account
Rare object access attempts by an account
Abnormal number of hosts accessed-SIEM-17
Abnormal number of administrative share object accessed-SIEM-17

COUNT (resourcecustomfield5)
DISTCOUNT (resourcecustomfield5)

Abnormal Number of Failed Logons from an IP Address–SIEM–13

Criticality: Low
Applies to: Functionality
Policy Category: Alert

Device Category
Windows

Description
High number of failed logons observed from an ipaddress

Analytical Type
Directive Based

Prerequisites
- windows logs
- IP data
- CMDB data / host naming convention

Violation Entity
Network Address

Threat Focus Area
Cyber

Threat Indicator
High number of accounts from the same ipaddress for authentication failures or lockout events

Kill Chain Stage
Recon

Remediation Steps
Possible further analysis/triage steps to consider:

1. Determine if the Source is a Virtual Desktop Server/SCCM server.
2. Determine if any of the accounts have a peer commonality.
3. Determine if any of the accounts and peers (if peer connection identified) had successful logins.
4. Determine if the host has any other anomalies

Possible Remediation steps after further analysis/triage:

1. Open ticket to add server to whitelist / Criteria to Filter event to stop future false positives.
2. If successful logins observed, Open ticket to Disable and reset password for accounts as they could be compromised.
3. If host found to be malicious, Open ticket to Isolate / remediate system according to internal Incident Response playbook.

Detection Algorithm
Aggregated Event Analytics

Criteria to Filter Event
baseeventid equal to 4625 [or]

baseeventid equal to 529 [or]
baseeventid equal to 4771
AND
ipaddreess not equal to - [and]
ipaddress not equal to 0.0.0.0 [and]
resourcename does not contain ADS [and]
resourcename does not contain ADC [and]
account name not equal to - [and]
account name does not contain SYSTEM [and]
account name does not contain $ [and]
account name does not contain ANONYMOUS LOGON [and]
account name does not contain Window Manager

Directives

Name FailedLogonsFromIP
Filter for Events matching criteria? baseeventid CONDITION_EQUALS 4625 OR
baseeventid CONDITION_EQUALS 529 OR
baseeventid CONDITION_EQUALS 4771
Having similar ipaddress
Number of Occurrences 5
Within Duration 00:30:00
Should events happen consecutively? false
Distinct? accountname

Risk Boosters

Match Criteria:
baseeventid equal to 4625 [or]
baseeventid equal to 529 [or]
baseeventie equal to 4771
increase factor 1,.0

Verbose Info

Accounts: ${accountname$LIST!"UNKNOWN"} failed authentication from IP address:
${ipaddress!"UNKNOWN"} Message: ${message!"UNKNOWN"} EventID: ${baseeventid!"UNKNOWN"}
Host: ${destinationhostname!"UNKNOWN"}

Response Bot Fields/Attributes/Policies

Abnormal number of account lockouts-SIEM-13
Abnormal number of kerberos pre authentication failures-SIEM-13
Abnormal number of logon failures-SIEM-13
Abnormal number of remote logon attempts-SIEM-13
Abnormal number of logon failures from an account-SIEM-13
Abnormal number of failed logons on a resource- SIEM-13
Multiple failed logons
Possible password spraying from an ipaddress
Possible password spraying from a resource
Abnormal number of account lockout events
Abnormal number of kerberos pre authentication failures
High number of accounts from the same ipaddress for authentication failures or lockout events
Abnormal number of logon failures
Rare host accessed by an account - Logon Failure
High Number of Failed Logins from an Undocumented Account
Windows Account lockouts
Abnormal number of account lockouts-SIEM-17
Abnormal number of kerberos pre authentication failures-SIEM-17
Abnormal number of failed logons on a resource- SIEM-17
Abnormal number of failed logons from an ipaddress-SIEM-17

Abnormal Number of Failed Logons on a Resource–SIEM–13

Criticality: Low
Applies to: Functionality
Policy Category: Alert

Device Category

Windows

Description

High number of failed logons observed from a resource

Analytical Type

Directive Based

Prerequisites

- windows logs
- CMDB data / host naming convention

Violation Entity

Resources

Threat Indicator

Possible Bruteforce

Kill Chain Stage

Recon

Remediation Steps

Possible further analysis/ triage steps to consider:

1. Determine if the Source is a Virtual Desktop Server / SCCM server.
2. Determine if any of the accounts have a peer commonality.
3. Determine if any of the accounts and peers (if peer connection identified) had successful logins.
4. Determine if the host has any other anomalies

Possible Remediation steps after further analysis/triage:

1. Open ticket to add server to whitelist / Criteria to Filter event to stop future false positives.
2. f successful logins observed, Open ticket to Disable and reset password for accounts as they could be compromised.
3. If host found to be malicious, Open ticket to Isolate / remediate system according to internal Incident Response playbook.

Detection Algorithm

Aggregated Event Analytics

Criteria to Filter Event

Source HostName IS NOT NULL
Source HostName NOT EQUAL TO -
Source HostName NOT EQUAL TO localhost
baseeventid EQUAL TO 4625
Source HostName DOES NOT CONTAIN ADS
Source HostName DOES NOT CONTAIN ADC

Account Name NOT EQUAL TO NA
Account Name NOT EQUAL TO -
Account Name DOES NOT CONTAIN SYSTEM
Account Name NOT EQUAL TO ANONYMOUS LOGON
Account Name DOES NOT CONTAIN $
Account Name DOES NOT CONTAIN DWM

Directives

Name abnormal number of failed logon from resource
Filter for Events matching criteria? NA
Having similar resourcename
Number of Occurrences 5
Within Duration 00:30:00
Should events happen consecutively? false
Distinct? accountname

Risk Boosters

Match Criteria:
baseeventid equal to 4625 increase factor 1.0

Verbose Info

Accounts: ${accountname$LIST!"UNKNOWN"} failed to logon to Host: ${destinationhostname!"UNKNOWN"} with Logon Type: ${customnumber1!"UNKNOWN"} from IP address: ${ipaddress!"UNKNOWN"} Message: ${message!"UNKNOWN"} EventID: ${baseeventid!"UNKNOWN"}

Response Bot Fields/Attributes/Policies

Abnormal number of account lockouts-SIEM-13
Abnormal number of remote interactive logon from an account-SIEM-13
Abnormal number of failed logons from an ipaddress-SIEM-13
Abnormal number of logon failures-SIEM-13
Abnormal number of kerberos pre authentication failures-SIEM-13
Abnormal number of remote logon attempts-SIEM-13
Abnormal number of logon failures from an account-SIEM-13
Multiple failed logons
Possible remote interactive logon enumeration
Possible password spraying from an ipaddress
Possible password spraying from a resource
Abnormal number of account lockout events
Abnormal number of kerberos pre authentication failures
High number of accounts used on a workstation for successful authentications or run as events
High number of accounts from the same ipaddress for successful authentications or run as events
High number of accounts from the same ipaddress for authentication failures or lockout events
Abnormal number of logon failures
Suspicious Logon Attempts
Abnormal number of remote logon attempt
Abnormal number of successful authentication attempts
High Number of Failed Logins from an Undocumented Account
Abnormal number of remote logon attempts
Suspicious Account Activity - Peak Credential Validation Failure Increase For Host Analytic
Abnormal number of account lockouts-SIEM-17
Abnormal number of failed logons from an ipaddress-SIEM-17
Abnormal number of kerberos pre authentication failures-SIEM-17
Abnormal number of failed logons on a resource- SIEM-17

Abnormal Number of Hosts Accessed

Criticality: Low

Applies to: Functionality
Policy Category: Alert

Device Category
Windows

Description
High number of hosts accessed during successful authentication events or run-as events may be indicative of malicious insider/cyber laterally propagating across multiple hosts using elevated credentials.

Technique Used
Enumeration Behavior anomaly for hosts accessed

Analytical Type
Tier 2 Behavior Summary

Prerequisites
- windows logs
- Behavior profiles
- Naming conventions for hosts

Violation Entity
Resource Group Account

Threat Focus Area
Cyber

Threat Indicator
Lateral Movement

Kill Chain Stage
Execute

Remediation Steps
Possible steps for further analysis / triage to consider:

1. Determine if the activity is approved by:
    - Checking service management system for an incident / work order (ticket) associated with the activity
    - Comparison to the user's peer group
    - Role to privilege comparison
2. Determine if the target accounts and resources have additional anomalies
3. Determine if the source account has other anomalies.
4. Determine if the endpoint has other anomalies associated with its processes, sessions, or network connections.

Possible Remediation steps after further analysis and triage:

1. Submit a ticket to revert any changes that occurred.
2. Submit a ticket to reset passwords / disable the account(s).
3. Submit a ticket to remove the account(s) (as needed)
4. Submit a ticket to revoke privileges
5. Submit a ticket to perform a full Antivirus scan
6. Submit a ticket for host isolation and further remediation as per internal **IR playbooks dictate.**

Detection Algorithm

Enumeration Behavior
Features:
- baseeventid
- destinationusername
- transactionstring1

Distinct Destination hostname
Daily Count of host accessed during successful authentication-9
Flagged Self
Distinct transaction occurence Abnormally higher than users daily behavior
Sigma Threshold 0.5

Criteria to Filter Event

Account Name IS NOT NULL [and]
baseeventid EQUAL TO 4624 [and]
Account Name DOES NOT CONTAIN $
OR
baseeventid EQUAL TO 4648 [or]
baseeventid EQUAL TO 4776
OR
baseeventid EQUAL TO 528 [and]
Account Name DOES NOT CONTAIN $

Verbose Info

Account ${accountname!"ACCOUNTNAME"} accessed Destination Hosts: ${destinationhostname$LIST!"UNKNOWN"} from IP address: ${ipaddress!"UNKNOWN"} Host: ${resourcename!"UNKNOWN"} Message: ${message!"UNKNOWN"} EventID: ${baseeventid!"UNKNOWN"}

Response Bot Fields/Attributes/Policies

Rare host accessed by an account
Abnormal number of host access attempts
Rare host accessed by an account - Logon Success
Suspicious host access behavior from an account
Abnormal object or network share access attempts by resource-SIEM-13
Abnormal number of administrative share object accessed-SIEM-13
Abnormal number of hosts accessed-SIEM-13
Abnormal object or network share access attempts-SIEM-13
Rare admin share access by an account
Abnormal number of network share object access
Abnormal number of administrative share object accessed
Spike in administrative shares accessed
Rare host accessed by an account - Logon Failure
Rare Host Accessed Attempt By Account
Unusual high number of network shares accessed - SIEM
Rare Host Accessed from an Account
Rare object access attempts by an account
Abnormal number of administrative share object accessed-SIEM-17
Abnormal number of hosts accessed-SIEM-17

Abnormal Number of Remote Interactive Logon from an Account–SIEM–13

Criticality: Low
Applies to: Functionality

Policy Category: Alert

Device Category
Windows

Description
Anomalous number of remote interactive logon from an account

Analytical Type
Directive Based

Prerequisites
- windows logs
- user HR data
- user naming convention
- Host naming convention

Violation Entity
Resource Group Account

Threat Indicator
Possible Account Takeover

Kill Chain Stage
Recon

Remediation Steps
Possible steps for further analysis / triage to consider:

1. Determine if the activity is approved by:
    - Checking service management system for an incident / work order (ticket) associated with the activity
    - Comparison to the user's peer group
    - Role to privilege comparison
2. Determine if the target accounts have any anomalies
3. Determine if the source account has other anomalies.
4. Determine if the endpoint has other anomalies associated with its processes, sessions, or network connections.

Possible Remediation steps after further analysis and triage:

1. Submit a ticket to reset passwords / disable the account(s).
2. Submit a ticket to remove the account(s) (as needed)
3. Submit a ticket to revoke privileges
4. Submit a ticket to perform a full Antivirus scan
5. Submit a ticket for host isolation and further remediation as per internal IR playbooks dictate

Note:

- Desktop Support / Network Engineers / Administrators will likely trigger this event from time to time due to need to make changes or login to multiple devices in an environment in a short time. So verify if this is the case before escalation**.**

Detection Algorithm
Aggregated event analytics

Criteria to Filter Event

baseeventid EQUAL TO 4624 [or]
baseeventid EQUAL TO 528
AND
Account Name NOT EQUAL TO - [and]
Account Name IS NOT NULL [and]
Account Name NOT EQUAL TO ANONYMOUS LOGON [and]
Account Name DOES NOT CONTAIN $ [and]
Account Name DOES NOT CONTAIN SYSTEM [and]
Account Name NOT EQUAL TO NA [and]
Account Name DOES NOT CONTAIN Window Manager [and]
Account Name DOES NOT CONTAIN DWM [and]
CustomNumber 1 EQUAL TO 10.0

Directives

Name RemoteInteractiveLogons
Filter for Events matching criteria? eventid CONDITION_EQUALS 4624 AND customnumber1 CONDITION_EQUALS 10.0
Having similar accountname
Number of Occurrences 5
Within Duration 01:00:00
Should events happen consecutively? false
Distinct? destinationhostname

Verbose Info

Account: ${accountname!"ACCOUNTNAME"} IP address: ${ipaddress$LIST!"UNKNOWN"} Host: ${resourcename$LIST!"UNKNOWN"} Message: ${message!"UNKNOWN"} EventID: ${baseeventid!"UNKNOWN"}

Response Bot Fields/Attributes/Policies

Abnormal number of remote logon attempts
Remote interactive logon to domain controller by non-admin account
Abnormal number of remote logon attempt
Abnormal number of remote logon attempts-SIEM-13

Abnormal Object or Network Share Access Attempts by Resource–SIEM–13

Criticality: Low
Applies to: Functionality
Policy Category: Alert

Device Category

Windows

Description

Detects multiple network object access that could indicate an attacker snooping and collecting data for exfiltration.

Analytical Type

Directive Based

Prerequisites

- windows logs
- Host naming convention

Violation Entity
Resources

Threat Focus Area
Insider/Cyber

Threat Indicator
Suspicious Network Share Access

Kill Chain Stage
Recon

Remediation Steps
Possible steps for further analysis / triage to consider:

1. Determine if the activity is approved by:
    - Checking service management system for an incident / work order (ticket) associated with the activity
    - Comparison to the user's peer group
    - Role to privilege comparison
2. Determine if the source account has other anomalies.
3. Determine if the endpoint has other anomalies associated with its processes, sessions, or network connections.

Possible Remediation steps after further analysis and triage:

1. Submit a ticket to revert any changes that occurred.
2. Submit a ticket to reset passwords / disable the account(s).
3. Submit a ticket to remove the account(s) (as needed)
4. Submit a ticket to revoke privileges
5. Submit a ticket to perform a full Antivirus scan
6. Submit a ticket for host isolation and further remediation as per internal IR playbooks dictate.

Detection Algorithm
Aggregated event analytics

Criteria to Filter Event
resourcename IS NOT NULL [and]
resourcename NOT EQUAL TO - [and]
resourcename NOT EQUAL TO localhost [and]
baseeventid EQUAL TO 5140
AND
Account Name NOT EQUAL TO - [and]
Account Name DOES NOT CONTAIN LOCAL [and]
Account Name DOES NOT CONTAIN ANONYMOUS [and]
Account Name DOES NOT CONTAIN $

Directives
Name High network shares-access
Filter for Events matching criteria? NA
Having similar resourcename
Number of Occurrences 5
Within Duration 00:30:00
Should events happen consecutively? false
Distinct? accountname

Risk Boosters
Match criteria:
baseeventid equal to 5140 increase factor 1.0

Verbose Info
Account: ${accountname!"ACCOUNTNAME"} IP address: ${ipaddress!"UNKNOWN"} Host: ${resourcename!"UNKNOWN"} Destination User: ${destinationusername!"UNKNOWN"} Message: ${message!"UNKNOWN"} EventID: ${baseeventid!"UNKNOWN"}

Response Bot Fields/Attributes/Policies
Abnormal number of administrative share object accessed-SIEM-13
Abnormal object or network share access attempts-SIEM-13
Rare admin share access by an account
Abnormal number of network share object access
Abnormal number of administrative share object accessed
Spike in administrative shares accessed
Unusual high number of network shares accessed - SIEM
Abnormal number of administrative share object accessed-SIEM-17
Rare host accessed by an account
Abnormal number of host access attempts
Rare host accessed by an account - Logon Success
Rare host accessed by an account - Logon Failure
Rare Host Accessed Attempt By Account
Rare Host Accessed from an Account
Suspicious host access behavior from an account

Audit Policy Changes
Criticality: None
Applies to: Functionality
Policy Category: Alert

Device Category
Windows

Description
This may be indicative of an audit log tampering activity

Analytical Type
Real Time Policy

Technique Used
Behavior anomaly on audit log clearing activity.

Prerequisites
- windows logs
- user naming convention

Violation Entity
Activity Account

Threat Focus Area
Insider/Cyber

Threat Indicator
Possible privilege MISUSE

Kill Chain Stage
Delivery

Remediation Steps
Possible steps for further analysis / triage to consider:

1. Determine if the activity is approved by:
    - Checking service management system for an incident / work order (ticket) associated with the activity
    - Comparison to the user's peer group
    - Role to privilege comparison
2. Determine if the account has other anomalies

Possible Remediation steps after further analysis and triage:

3. Submit a ticket to revert any changes made.
4. Submit a ticket to reset password / disable the source account.
5. Submit a ticket to revoke privileges
6. Submit a ticket to execute internal IR Playbook

Detection Algorithm
Individual Event Analytics

Criteria to Filter Event
baseeventid EQUAL TO 4912
AND
Account Name DOES NOT CONTAIN $ [and]
Account Name DOES NOT CONTAIN ANONYMOUS [and]
Account Name DOES NOT CONTAIN LOCAL [and]
Account Name NOT EQUAL TO -

Verbose Info
Account: ${accountname!"ACCOUNTNAME"} IP address: ${ipaddress!"UNKNOWN"} Host: ${resourcename!"UNKNOWN"} Destination User: ${destinationusername!"UNKNOWN"} Message: ${message!"UNKNOWN"} EventID: ${baseeventid!"UNKNOWN"}

Response Bot Fields/Attributes/Policies
Rare audit log clearing by an account
Rare regedit usage compared to peer
Rare registry modification by an account
Audit Log Tampering
Suspicious AD policy change
Suspicious Registry Modification Observed
Firewall disabled on windows

Certificate Service Status
Criticality: None
Applies to: Functionality
Policy Category: Alert

Device Category
Windows

Description
A certificate service stopped could indicate malicious activity. This should be coupled with other endpoint, authentication or network anomalies.

Analytical Type
Real Time Policy

Technique Used
Behavior anomaly.

Prerequisites
- windows logs
- user naming convention

Violation Entity
Activity Account

Threat Focus Area
Cyber

Threat Indicator
Suspicious Process execution

Kill Chain Stage
Execute

Remediation Steps
Possible steps for further analysis / triage to consider:

1. Determine if the activity is approved by:
    - Checking service management system for an incident / work order (ticket) associated with the activity
    - Comparison to the user's peer group
    - Role to privilege comparison
2. Determine if the account has other anomalies

Possible Remediation steps after further analysis and triage:

3. Submit a ticket to revert any changes made.
4. Submit a ticket to reset password / disable the source account.
5. Submit a ticket to revoke privileges
6. Submit a ticket to execute internal IR Playbook

Detection Algorithm
Individual Event Analytics

Criteria to Filter Event
baseeventid EQUAL TO 4881 [and]
AND

Account Name DOES NOT CONTAIN $ [and]
Account Name DOES NOT CONTAIN LOCAL [and]
Account Name DOES NOT CONTAIN ANONYMOUS [and]
Account Name NOT EQUAL TO - [and]

Verbose Info
Account: ${accountname!"ACCOUNTNAME"} IP address: ${ipaddress!"UNKNOWN"} Host: ${resourcename!"UNKNOWN"} Destination User: ${destinationusername!"UNKNOWN"} Message: ${message!"UNKNOWN"} EventID: ${baseeventid!"UNKNOWN"}

Response Bot Fields/Attributes/Policies
Rare process creation on an endpoint
Rare Basic Service Operation
Rare token elevation for process
Rare process spawned by a parent process
Suspicious Process Activity - Log Clearing Analytics
Suspicious Process Activity - Potential Mimikatz or Hash Passing Token Creation - Powershell Privileged Service Call Analytic
Suspicious Process Activity - Endpoint - Potential Mimikatz Object Handling Activity Analytic

---

Logging User Account Disabled
Criticality: None
Applies to: Functionality
Policy Category: Alert

Device Category
Windows

Description
Monitors disabling of service accounts used for logging purposes

Analytical Type
Real Time Policy

Technique Used
Behavior anomaly on service accounts used for logging

Prerequisites
- windows logs
- IP atributions
- Naming Conventions

Violation Entity
Resource Group Account

Threat Focus Area
Insider/Cyber

Threat Indicator
Suspicious User management event detected

Kill Chain Stage
Recon

Remediation Steps

- Nessus LaunchScan
- NessusConnector StopScan
- NessusConnector FetchScan
- AD BlockUser
- AD UnBlockUser
- Tanium - Machine Information
- Tanium - Running Processes with MD5
- Tanium - Running Applications
- Tanium - Non-approved Established Connections

Detection Algorithm

Individual Event Analytics

Criteria to Filter Event

baseid equal to 4725
AND
Account Name NOT EQUAL TO - [and]
Account Name DOES NOT CONTAIN $ [and]
Account Name DOES NOT CONTAIN LOCAL [and]
Account Name DOES NOT CONTAIN ANONYMOUS

Verbose Info

Account: ${accountname!"ACCOUNTNAME"} IP address: ${ipaddress!"UNKNOWN"} Host: ${resourcename!"UNKNOWN"} Destination User: ${destinationusername!"UNKNOWN"} Message: ${message!"UNKNOWN"} EventID: ${baseeventid!"UNKNOWN"}

Response Bot Fields/Attributes/Policies

Rare registry modification by an account
Audit policy changes
Suspicious AD policy change

Multiple Failed Logons

Criticality: None
Applies to: Functionality
Policy Category: Alert

Device Category

Windows

Description

Repeated failed authentication events may be indicative of a malicious entity attempting to communicate to a Command and Control server or to receiving the malicious payload.

Analytical Type

Directive Based

Technique Used

Aggregated event analysis on failed authentication events
Type : SIEM

Prerequisites
- windows logs

Violation Entity
Activity Account

Threat Focus Area
Cyber

Threat Indicator
Possible bruteforce

Kill Chain Stage
Recon

Remediation Steps
- Nessus LaunchScan
- NessusConnector StopScan
- NessusConnector FetchScan
- AD BlockUser
- AD UnBlockUser
- Tanium - Machine Information
- Tanium - Running Processes with MD5
- Tanium - Running Applciations
- Tanium - Non-approved Established Connections

Criteria to Filter Event
baseevent id equal to 4625

Directives
Name Failed Events
Filter for Events matching criteria? baseeventid CONDITION_EQUALS 4625
Having similar accountname
Number of Occurrences 15
Within Duration 00:15:00
Should events happen consecutively? false
Distinct? NA

Verbose Info
Account ${accountname!"ACCOUNTNAME"} performed multiple failed logon attempts

Response Bot Fields/Attributes/Policies
Abnormal number of account lockouts-SIEM-13
Abnormal number of remote interactive logon from an account-SIEM-13
Abnormal number of failed logons from an ipaddress-SIEM-13
Abnormal number of logon failures-SIEM-13
Abnormal number of remote logon attempts-SIEM-13
Abnormal number of logon failures from an account-SIEM-13
Abnormal number of failed logons on a resource- SIEM-13
Abnormal number of logon failures
Abnormal number of remote logon attempt
Abnormal number of remote logon attempts

Abnormal number of account lockouts-SIEM-17
Abnormal number of failed logons from an ipaddress-SIEM-17
Abnormal number of failed logons on a resource- SIEM-17
Abnormal number of failed logins for an account

Possible Bruteforce Attempt–13

Criticality: None
Applies to: Functionality
Policy Category: Alert

Device Category

Windows

Description

Failed logon attempts followed by successful logons

Analytical Type

Directive Based

Prerequisites

- windows logs
- ip attribution

Violation Entity

Resource Group Account

Threat Focus Area

Cyber

Threat Indicator

Possible bruteforce

Kill Chain Stage

Recon

Remediation Steps

- Nessus LaunchScan
- NessusConnector StopScan
- NessusConnector FetchScan
- AD BlockUser
- AD UnBlockUser
- Tanium - Machine Information
- Tanium - Running Processes with MD5
- Tanium - Running Applciations
- Tanium - Non-approved Established Connections

Detection Algorithm

Aggregated Event Analytics

Criteria to Filter Event

Account Name NOT EQUAL TO - [and]
CustomNumber 1 IS NOT NULL [and]

IPAddress IS NOT NULL [and]
IPAddress NOT EQUAL TO 0.0.0.0 [and]
Account Name DOES NOT CONTAIN $ [and]
Account Name NOT EQUAL TO ANONYMOUS LOGON [and]
Account Name NOT EQUAL TO NA [and]
Account Name DOES NOT CONTAIN SYSTEM [and]
Account Name DOES NOT CONTAIN Window Manager [and]
Account Name DOES NOT CONTAIN DWM
AND
baseeventid EQUAL TO 4624 [or]
baseeventid EQUAL TO 528 [or]
baseeventid EQUAL TO 4625 [or]
baseeventid EQUAL TO 4771 [or]
baseeventid EQUAL TO 4769 [or]
baseeventid EQUAL TO 540

Directives

Parent
Name BruteforceAttempt
Filter for Events matching criteria? baseeventid CONDITION_EQUALS 4625 OR baseeventid CONDITION_EQUALS 4771
Having similar accountname
Number of Occurrences 5
Within Duration 00:10:00
Should events happen consecutively? false
Distinct? NA

Child
Name SuccessfulLogin
Filter for Events matching criteria? baseeventid CONDITION_EQUALS 4769 OR baseeventid CONDITION_EQUALS 4624
Number of Occurrences 1
Within Duration 00:10:00
Should events happen consecutively? false
Distinct? NA
Minimum duration between parent and child 00:10:00
Common between parent and child? Accountname

Risk Boosters

Match Criteria:
baseeventid equal to 4771 [or]
baseeventid equal to 4625
increase factor 5.0

Verbose Info

Account: ${accountname!"ACCOUNTNAME"} IP address: ${ipaddress!"UNKNOWN"} Host: ${resourcename!"UNKNOWN"} Destination User: ${destinationusername!"UNKNOWN"} Message: ${message!"UNKNOWN"} EventID: ${baseeventid!"UNKNOWN"}

Response Bot Fields/Attributes/Policies

Abnormal number of account lockouts-SIEM-13
Abnormal number of logon failures from an account-SIEM-13
Abnormal number of failed logons on a resource- SIEM-13
Abnormal number of account lockout events
High number of accounts from the same ipaddress for authentication failures or lockout events
Abnormal number of logon failures

High Number of Failed Logins from an Undocumented Account
Windows Account lockouts
Possible Brute Force Attack VPN
Abnormal number of account lockouts-SIEM-17
Abnormal number of failed logins for an account

Remote Interactive Logon to Domain Controller by Non-Admin Account

Criticality: Low
Applies to: Functionality
Policy Category: Alert

Device Category

Windows

Description

Detects remote logins to domain controllers by non-admins accounts that could indicate an attacker performing recon to determine what entity to move to next in the environment.

Analytical Type

Real Time Policy

Prerequisites

- windows logs

Violation Entity

Resource Group Account

Threat Focus Area

Insider/Cyber

Threat Indicator

Possible unauthorized access

Kill Chain Stage

Recon

Remediation Steps

- AD BlockUser
- AD UnBlockUser
- Tanium - Machine Information
- Tanium - Running Processes with MD5
- Tanium - Running Applciations
- Tanium - Non-approved Established Connections

Detection Algorithm

Individual Event Analytics

Criteria to Filter Event

baseeventid EQUAL TO 4624 [or]

baseeventid EQUAL TO 528
AND
CustomNumber 1 CONTAINS 10
AND
Account Name DOES NOT END WITH -a [and]
Account Name DOES NOT END WITH -da [and]
Account Name DOES NOT END WITH -na [and]
Account Name DOES NOT END WITH -sda [and]
Account Name DOES NOT END WITH -sa [and]
Account Name DOES NOT END WITH PA [and]
Account Name NOT EQUAL TO ANONYMOUS LOGON
AND
Destination HostName CONTAINS ADS [or]
Destination HostName CONTAINS ADC

Verbose Info

Account: ${accountname!"ACCOUNTNAME"} IP address: ${ipaddress!"UNKNOWN"} Host: ${resourcename!"UNKNOWN"} Destination User: ${destinationusername!"UNKNOWN"} Message: ${message!"UNKNOWN"} EventID: ${baseeventid!"UNKNOWN"}

Response Bot Fields/Attributes/Policies

Abnormal number of remote interactive logon from an account-SIEM-13
Abnormal number of remote logon attempts-SIEM-13
Rare admin share access by an account
Rare target account authentication using explicit credentials
Abnormal number of remote logon attempt
Rare host accessed by an account - Logon Success
Rare host accessed by an account - Logon Failure
Abnormal number of remote logon attempts
Rare Host Accessed from an Account
Suspicious host access behavior from an account

Restricted Group Change

Criticality: Low
Applies to: Functionality
Policy Category: Alert

Device Category

Windows

Description

These restricted group change events may be indicative of a possible backdoor access attempt.

Analytical Type

Real Time Policy

Technique Used

Entity attribution.

Prerequisites

- windows logs

Violation Entity

Activity Account

Threat Focus Area
Cyber

Threat Indicator
Suspicious group management event detected

Kill Chain Stage
Recon

Remediation Steps
- AD BlockUser
- AD UnBlockUser
- Tanium - Machine Information
- Tanium - Running Processes with MD5
- Tanium - Running Applciations
- Tanium - Non-approved Established Connections

Detection Algorithm
Individual Event Analytics

Criteria to Filter Event

baseeventid EQUAL TO 1202
AND
Account Name NOT EQUAL TO - [and]
Account Name DOES NOT CONTAIN LOCAL [and]
Account Name DOES NOT CONTAIN ANONYMOUS [and]
Account Name DOES NOT CONTAIN $

Verbose Info
Account ${accountname!"ACCOUNTNAME"} performed ${transactionstring1!"ACTIVITY"} from ipaddress ${ipaddress!"UNKNOWN"}

Response Bot Fields/Attributes/Policies
A member was added and removed from a security enabled group within a short time-13
Account added and removed to security group
Member added to built-in admin groups by uncorelated accounts
Rare builtin member group additions
Rare admin group member additions by user compared to peer
A member was added and removed from a security enabled group within a short time-17
Possible AD Enumeration
Rare privilege enumeration event
Abnormal number of account enumeration attempts on an endpoint
Possible Privilege Enumeration
Suspicious AD Enumeration Observed
Possible Privilege Escalation - Self Escalation
Abnormal number of privileges enumerated

Suspicious Logon Attempts
Criticality: None
Applies to: Functionality
Policy Category: Alert

Device Category
Windows

Description
Sysadmin authentication could indicate a malicious activity.

Analytical Type
Real Time Policy

Technique Used
Behavior anomaly on accounts with admin privileges

Prerequisites
- windows logs

Violation Entity
Activity Account

Threat Focus Area
Cyber

Threat Indicator
Suspicious AD Authentication

Kill Chain Stage
Recon

Remediation Steps
- AD BlockUser
- AD UnBlockUser
- Tanium - Machine Information
- Tanium - Running Processes with MD5
- Tanium - Running Applciations
- Tanium - Non-approved Established Connections

Detection Algorithm
Individual Event Analytics

Criteria to Filter Event
baseeventid EQUAL TO 4624
AND
Account Name STARTS WITH AD- [and]
Account Name ENDS WITH -SA

Verbose Info
Account: ${accountname!"ACCOUNTNAME"} IP address: ${ipaddress!"UNKNOWN"} Host: ${resourcename!"UNKNOWN"} Destination User: ${destinationusername!"UNKNOWN"} Message: ${message!"UNKNOWN"} EventID: ${baseeventid!"UNKNOWN"}

Response Bot Fields/Attributes/Policies
Abnormal number of remote interactive logon from an account-SIEM-13

Abnormal number of logon failures-SIEM-13
Abnormal number of remote logon attempts-SIEM-13
Abnormal number of logon failures from an account-SIEM-13
Multiple failed logons
Abnormal number of logon failures
Abnormal number of remote logon attempt
Rare host accessed by an account - Logon Success
Rare host accessed by an account - Logon Failure
Abnormal number of successful authentication attempts
Abnormal number of remote logon attempts
Use of explicit credentials - Account sharing or Password misuse
Abnormal number of process execution using explicit credentials
High number of accounts from the same ipaddress for authentication failures or lockout events
High number of accounts from the same ipaddress for successful authentications or run as events
High number of accounts used on a workstation for successful authentications or run as events
Rare target account authentication using explicit credentials
Rare process detected for authentication using explicit credentials
High Number of Failed Logins from an Undocumented Account

Suspicious Process Activity–Log Clearing Analytics

Criticality: Low
Applies to: Functionality
Policy Category: Alert

Device Category
Windows

Description
Generates a violation when event logs are cleared

Analytical Type
Real Time Policy

Prerequisites
- windows logs

Violation Entity
Activity Account

Threat Focus Area
Cyber

Threat Indicator
Suspicious process execution

Kill Chain Stage
Execute

Remediation Steps
- Nessus LaunchScan
- NessusConnector StopScan
- NessusConnector FetchScan
- AD BlockUser
- AD UnBlockUser

- Tanium - Machine Information
- Tanium - Running Processes with MD5
- Tanium - Running Applciations
- Tanium - Non-approved Established Connections

Detection Algorithm
Individual Event Analytics

Criteria to Filter Event
baseeventid EQUAL TO 4688 [and]
devicecustomstring4 CONTAINS wevtutil.exe cl

Verbose Info
Account ${accountname!"ACCOUNTNAME"} performed ${transactionstring1!"ACTIVITY"} from ipaddress ${ipaddress!"UNKNOWN"}

Response Bot Fields/Attributes/Policies
Rare process creation on an endpoint
Rare token elevation for process
Rare process spawned by a parent process
Rare process detected for authentication using explicit credentials
Audit Log Tampering
Rare audit log clearing by an account

Use of Any Default Credentials
Criticality: None
Applies to: Functionality
Policy Category: Alert

Device Category
Windows

Description
Detects any use of default credentials that can indicate account misuse or an attacker in the environment attempting to carry out objects on target.

Analytical Type
Real Time Policy

Prerequisites
- windows logs

Violation Entity
Activity Account

Threat Focus Area
Cyber

Threat Indicator
Possible unauthorized access

Kill Chain Stage
Recon

Remediation Steps
- AD BlockUser
- AD UnBlockUser
- Tanium - Machine Information
- Tanium - Running Processes with MD5
- Tanium - Running Applciations
- Tanium - Non-approved Established Connections
- Tanium - User Sessions

Detection Algorithm
Individual Event Analytics

Criteria to Filter Event
Account Name EQUAL TO root [or]
Account Name EQUAL TO admin [or]
Account Name EQUAL TO administrator [or]
Account Name EQUAL TO guest [or]
Account Name EQUAL TO svc

Verbose Info
Account: ${accountname!"ACCOUNTNAME"} IP address: ${ipaddress!"UNKNOWN"} Host: ${resourcename!"UNKNOWN"} Destination User: ${destinationusername!"UNKNOWN"} Message: ${message!"UNKNOWN"} EventID: ${baseeventid!"UNKNOWN"}

Response Bot Fields/Attributes/Policies
Account added and removed to security group
Account Created and Deleted
Local accounts created on windows - Target domain analysis
Use of explicit credentials - Account sharing or Password misuse
Rare audit log clearing by an account
Rare registry modification by an account
New admin account detected
Rare local account created
Member added to built-in admin groups by uncorelated accounts
Rare target account authentication using explicit credentials
Rare builtin member group additions
Possible local account created
Suspicious Account Activity - Potential pass-the-hash - Host Length Analytic
Suspicious Account Activity - Kerberoasting - Rare TGS Encryption Type For User Analytic
Suspicious Account Activity - Kerberoasting - Peak TGS Request For User Analytic
Suspicious Process Activity - Log Clearing Analytics
Suspicious Process Activity - Potential Mimikatz or Hash Passing Token Creation - Powershell Privileged Service Call Analytic
Suspicious Process Activity - Endpoint - Potential Mimikatz Object Handling Activity Analytic
- Genertated by what i would likely do with a degault account

---

Windows Account Lockouts
Criticality: None
Applies to: Functionality
Policy Category: Alert

Device Category
Windows

Description
Detects multiple account lockouts that can indicate a denial of service by an attacker.

Analytical Type
Real Time Policy

Prerequisites
- windows logs

Violation Entity
Activity Account

Threat Focus Area
Insider/Cyber

Threat Indicator
Suspicious AD Authentication

Kill Chain Stage
Recon

Remediation Steps
1. Determine if the activity is approved by checking service management system for an incident/work order (ticket) associated with the activity.
2. Determine if the account has other anomalies.
3. Determine if the account or its peers have performed similar activities.
4. Determine if the account should be performing the activity via a role to privilege comparison.

For External IPs:
1. Determine is blacklisted or has Threat Intelligence associated with it.

For Internal IPs:
2. Determine if any of the processes and their hash values are malicious.

Possible Remediation steps after further analysis and triage:
3. Submit a ticket to revert any changes that occurred.
4. Submit a ticket to disable the account.
5. Submit a ticket to remove the account (as needed)
6. Submit a ticket to revoke privileges
7. Submit a ticket to block the IP and any other IPs/URLs found from Threat Intelligence lookup.
8. Submit a ticket to perform a full Antivirus scan
9. Submit a ticket for host isolation and further remediation as per internal IR playbooks dictate.

Detection Algorithm
IEE

Criteria to Filter Event
baseeventid EQUAL TO 4740 [and]
Account Name NOT EQUAL TO - [and]
Account Name DOES NOT CONTAIN SYSTEM [and]
Account Name NOT EQUAL TO NA [and]
Account Name NOT EQUAL TO ANONYMOUS LOGON [and]
Account Name DOES NOT CONTAIN WINDOW MANAGER [and]
Account Name DOES NOT CONTAIN DWM [and]

Account Name DOES NOT CONTAIN $

Verbose Info
Account: ${accountname!"ACCOUNTNAME"} IP address: ${ipaddress!"UNKNOWN"} Host: ${resourcename!"UNKNOWN"} Destination User: ${destinationusername!"UNKNOWN"} Message: ${message!"UNKNOWN"} EventID: ${baseeventid!"UNKNOWN"}

Response Bot Fields/Attributes/Policies
Abnormal number of logon failures from an account-SIEM-13
Rare interactive logon by service account
Windows activity by terminated accounts
Rare target account authentication using explicit credentials
High Number of Failed Logins from an Undocumented Account
Rare logon type detected for an account
VPN activity by undocumented accounts
Abnormal number of failed logins for an account

Windows Activity by Terminated Accounts
Criticality: None
Applies to: Functionality
Policy Category: Identity Issue

Device Category
Windows

Description
Activity by terminated users may be indicative of a possible account misuse or a gap in the deprovisioning process

Technique Used
Identity attribution

Analytical Type
Real Time Policy

Prerequisites
- windows logs

Violation Entity
Resource Group Account

Threat Focus Area
Insider/Cyber

Threat Indicator
Activity by terminated user

Kill Chain Stage
Exploit

Remediation Steps
- AD BlockUser
- AD UnBlockUser
- Tanium - Machine Information

- Tanium - Running Processes with MD5
- Tanium - Running Applciations
- Tanium - Non-approved Established Connections

Detection Algorithm
Individual Event Analytics

Criteria to Filter Event
STATUS EQUAL TO 0 [and]
baseeventid EQUAL TO 4624
or
STATUS EQUAL TO 0 [and]
baseeventid EQUAL TO 528
or
STATUS EQUAL TO 0 [or]
baseeventid EQUAL TO 540
or
Account Name DOES NOT CONTAIN $ [and]
Account Name NOT EQUAL TO - [and]
Account Name DOES NOT CONTAIN ANONYMOUS [and]
Account Name DOES NOT CONTAIN LOCAL

Verbose Info
Account: ${accountname!"ACCOUNTNAME"} IP address: ${ipaddress!"UNKNOWN"} Host: ${resourcename!"UNKNOWN"} Destination User: ${destinationusername!"UNKNOWN"} Message: ${message!"UNKNOWN"} EventID: ${baseeventid!"UNKNOWN"}

Response Bot Fields/Attributes/Policies
Account added and removed to security group
Rare target account authentication using explicit credentials
Rare logon type detected for an account
Web browsing activity from terminated accounts
VPN activity by terminated users
Email Sent by Terminated User

Possible Local Account Created
Criticality: None
Applies to: Functionality
Policy Category: Data Exfiltration

Device Category
Windows

Description
Accounts created on a rare domain could be possible local accounts and can't be monitored by the Domain Controller and which can be leveraged to avoid defense mechanisms or create backdoors for future malicious use.

Analytical Type
Traffic Analyzer

Prerequisites
- windows logs
- Behavior profiles

Violation Entity
Resource Group Account

Threat Focus Area
Insider/Cyber

Threat Indicator
Circumvention of controls

Kill Chain Stage
Recon

Remediation Steps
- VirusTotal ScanIP
- VirusTotal ScanURL
- VirusTotal ScanDomain
- Nessus LaunchScan
- NessusConnector StopScan
- NessusConnector FetchScan
- AD BlockUser
- AD UnBlockUser
- Tanium - Machine Information
- Tanium - Running Processes with MD5
- Tanium - Running Applciations
- Tanium - Non-approved Established Connections
- PassiveTotal - Get Passive DNS
- PassiveTotal - Get Subdomains
- PassiveTotal - Get Unique DNS
- PassiveTotal - Get Who Is
- PassiveTotal - Search Who is
- PassiveTotal - Search Who is by Keyword

Detection Algorithm
Traffic Analyzer

Criteria to Filter Event
baseeventid EQUAL TO 4720 [or]
baseeventid EQUAL TO 624
AND
Destination Network Domain IS NOT NULL [and]
Destination Network Domain NOT EQUAL TO - [and]
Destination Network Domain NOT EQUAL TO UNKNOWN [
AND
Account Name NOT EQUAL TO - [and]
Account Name DOES NOT CONTAIN LOCAL [and]
Account Name DOES NOT CONTAIN ANONYMOUS [and]
Account Name DOES NOT CONTAIN $

Additional Event Analytics
Detects when an account is created on non-approved domain and that domain is used as a destination for 10 events by said account

Directives
URL Visted by vistors
destination network domain account name 10

Verbose Info
Account: ${accountname!"ACCOUNTNAME"} IP address: ${ipaddress!"UNKNOWN"} Host: ${resourcename!"UNKNOWN"} Destination Domain: ${destinationntdomain!"UNKNOWN"} Message: ${message!"UNKNOWN"} EventID: ${baseeventid!"UNKNOWN"}

Response Bot Fields/Attributes/Policies
Uploads greater than 1MB to storage sites
Abnormal upload attempts to distinct storage sites
Uploads greater than 1MB to external sites
Abnormal amount of data uploads to storage sites
Abnormal amount of data uploads to external sites
Uploads to text storage websites
Uploads to news or media websites
Uploads to personal websites
Abnormal amount of data transmitted from known file transfer ports for IP address
Abnormal amount of data transmitted over covert channels for IP Address
Abnormal amount of data transmitted from known file transfer ports for Account
Abnormal amount of data transmitted over covert channels for Account
Detection of possible proxy circumvention
Traffic to known TOR exit nodes
Rare host accessed by an account
Rare host accessed by an account - Logon Success
Rare host accessed by an account - Logon Failure
Rare Host Accessed Attempt By Account
Rare Host Accessed from an Account
Suspicious host access behavior from an account
Unusual high number of network shares accessed - SIEM
Abnormal number of network share object access
Abnormal object or network share access attempts-SIEM-13
Abnormal object or network share access attempts by resource-SIEM-13

Abnormal Number of Host Access Attempts
Criticality: None
Applies to: Functionality
Policy Category: Data Exfiltration

Device Category
Windows

Description
High number of hosts accessed during failed authentication events or lockout events may be indicative of malicious insider/cyber attempting to laterally propagate across multiple hosts.

Technique Used
Enumeration Behavior anomaly for hosts accessed

Analytical Type
Tier 2 Behavior Summary

Prerequisites
- windows logs
- Behavior profiles

Violation Entity
Resource Group Account

Threat Focus Area
Cyber

Threat Indicator
Network Scanning and Enumeration

Kill Chain Stage
Recon

Remediation Steps
Possible steps for further analysis / triage to consider:

1. Determine if the activity is approved by:
    - Checking service management system for an incident / work order (ticket) associated with the activity
    - Comparison to the user's peer group
    - Role to privilege comparison
2. Determine if the target accounts and resources have additional anomalies
3. Determine if the source account has other anomalies.
4. Determine if the endpoint has other anomalies associated with its processes, sessions, or network connections.

Possible Remediation steps after further analysis and triage:

1. Submit a ticket to revert any changes that occurred.
2. Submit a ticket to reset passwords / disable the account(s).
3. Submit a ticket to remove the account(s) (as needed)
4. Submit a ticket to revoke privileges
5. Submit a ticket to perform a full Antivirus scan
6. Submit a ticket for host isolation and further remediation as per internal IR playbooks dictate.

Detection Algorithm
Enumeration Behavior
Features:
- baseeventid
- destinationusername
- transactionstring1

Distinct Destination hostname
Daily Count of Distinct hosts during authentication failures-9
Flagged Self
Distinct transaction occurence Abnormally higher than users daily behavior
Sigma Threshold 0.5

Criteria to Filter Event
baseeventid EQUAL TO 4625 [or]
baseeventid EQUAL TO 4740 [or]
baseeventid EQUAL TO 4771 [or]
baseeventid EQUAL TO 4776
AND
Account Name NOT EQUAL TO - [And]
Account Name DOES NOT CONTAIN $ [And]
Account Name DOES NOT CONTAIN LOCAL [And]
Account Name DOES NOT CONTAIN ANONYMOUS

Verbose Info
Account ${accountname!"ACCOUNTNAME"} attempted to access Destination Hosts: ${destinationhostname$LIST!"UNKNOWN"} from IP address: ${ipaddress!"UNKNOWN"} Host: ${resourcename!"UNKNOWN"} Message: ${message!"UNKNOWN"} EventID: ${baseeventid!"UNKNOWN"}

Response Bot Fields/Attributes/Policies
Abnormal number of hosts accessed-SIEM-13
Rare host accessed by an account
Abnormal number of hosts accessed
Rare host accessed by an account - Logon Success
Rare Host Accessed Attempt By Account
Rare Host Accessed from an Account
Abnormal object or network share access attempts by resource-SIEM-13
Abnormal object or network share access attempts-SIEM-13
Abnormal number of network share object access
Spike in administrative shares accessed
Rare host accessed by an account - Logon Failure
Suspicious host access behavior from an account
Rare object access attempts by an account
Abnormal number of administrative share object accessed-SIEM-17
Abnormal number of hosts accessed-SIEM-17

Rare Host Accessed by an Account– Logon Success
Criticality: None
Applies to: Functionality
Policy Category: Alert, Account Misuse

Device Category
Windows

Description
A spike in account accessing new hosts could indicate a possible account takeover or a lateral propagation attempt

Technique Used
Behavior anomaly on the hosts typically accessed by an account

Analytical Type
Tier 2 Behavior Summary

Prerequisites
- windows logs
- Behavior profiles

Violation Entity
Resource Group Account

Threat Focus Area
Insider/Cyber

Threat Indicator
Suspicious AD Authentication

Kill Chain Stage
Recon

Remediation Steps
- AD BlockUser
- AD UnBlockUser
- Tanium - Machine Information
- Tanium - Running Processes with MD5
- Tanium - Running Applciations
- Tanium - Non-approved Established Connections

Detection Algorithm
Rare Behavior

Criteria to Filter Event
baseeventid EQUAL TO 4624 [or]
baseeventid EQUAL TO 528 [or]
baseeventid EQUAL TO 540 [or]
baseeventid EQUAL TO 4776
AND
Account Name DOES NOT CONTAIN $ [and]
Account Name DOES NOT CONTAIN ANONYMOUS [and]
Account Name DOES NOT CONTAIN LOCAL [and]
Account Name NOT EQUAL TO -
AND
Destination HostName DOES NOT CONTAIN LDAP [and]
Destination HostName DOES NOT START WITH ADS [and]
Destination HostName DOES NOT START WITH ADC

Verbose Info
Account: ${accountname!"ACCOUNTNAME"} IP address: ${ipaddress!"UNKNOWN"} Host: ${resourcename!"UNKNOWN"} Message: ${message!"UNKNOWN"} EventID: ${baseeventid!"UNKNOWN"}

Response Bot Fields/Attributes/Policies
Abnormal number of administrative share object accessed-SIEM-13
Abnormal number of hosts accessed-SIEM-13
Abnormal object or network share access attempts-SIEM-13
Rare host accessed by an account
Rare admin share access by an account
Abnormal number of network share object access
Abnormal number of host access attempts
Abnormal number of hosts accessed
Abnormal number of administrative share object accessed
Spike in administrative shares accessed
Rare host accessed by an account - Logon Failure
Rare Host Accessed Attempt By Account
Unusual high number of network shares accessed - SIEM
Rare Host Accessed from an Account
Suspicious host access behavior from an account
Abnormal number of administrative share object accessed-SIEM-17
Abnormal number of hosts accessed-SIEM-17

Rare Service Created on Endpoint
Criticality: None

Applies to: Functionality
Policy Category: Account Misuse, Malware

Device Category
Windows

Description
This anomaly may be indicative of a possible malicious service being executed, additional indicators like path of execution would determine the severity.

Technique Used
Behavior anomaly on service created on an endpoint

Analytical Type
Tier 2 Behavior Summary

Prerequisites
- windows logs
- Behavior profiles

Violation Entity
Resource Group Account

Threat Focus Area
Cyber

Threat Indicator
Suspicious Process execution

Kill Chain Stage
Execute

Remediation Steps
- Nessus LaunchScan
- NessusConnector StopScan
- NessusConnector FetchScan
- AD BlockUser
- AD UnBlockUser
- Tanium - Machine Information
- Tanium - Running Processes with MD5
- Tanium - Running Applciations
- Tanium - Non-approved Established Connections

Detection Algorithm
Rare Behavior

Criteria to Filter Event
baseeventid EQUAL TO 592 [or]
baseeventid EQUAL TO 601 [or]
baseeventid EQUAL TO 4688 [or]
baseeventid EQUAL TO 4697
AND
Account Name DOES NOT CONTAIN $ [and]

Account Name DOES NOT CONTAIN ANONYMOUS [and]
Account Name DOES NOT CONTAIN LOCAL [and]
Account Name NOT EQUAL TO -

Verbose Info

Account: ${accountname!"ACCOUNTNAME"} IP address: ${ipaddress!"UNKNOWN"} Host: ${resourcename!"UNKNOWN"} Destination User: ${destinationusername!"UNKNOWN"} Message: ${message!"UNKNOWN"} EventID: ${baseeventid!"UNKNOWN"}

Response Bot Fields/Attributes/Policies

Rare process creation on an endpoint
Rare token elevation for process
Rare process spawned by a parent process
Rare process detected for authentication using explicit credentials
Suspicious Process Activity - Log Clearing Analytics
Suspicious Process Activity - Potential Mimikatz or Hash Passing Token Creation - Powershell Privileged Service Call Analytic
Suspicious Process Activity - Endpoint - Potential Mimikatz Object Handling Activity Analytic
Detection of possible backdoor
Use of credential dumpers
Rare Basic Service Operation
Suspicious Service creation
Unusual service authentication detected for user