Malicious Process Detected on attacker[.]ihatemikesimone[.]com

Report generated on 2025-10-03T15:35:57.313Z

Contents

Executive Summary

The incident titled "Malicious Process Detected on attacker[.]ihatemikesimone[.]com" was reported 2025-09-28T04:18:37.303Z.

- The status of the incident is open: investigating
- The incident has not been confirmed or analysed in Cisco XDR
- The likely cause of the incident is unknown

Further details about the incident reveal that:

- Number of devices involved in the incident: 6
- Number of users involved in the incident: 11
- Techniques used in the incident: OS Credential Dumping, OS Credential Dumping: LSASS Memory, System Service Discovery, System Network Configuration Discovery, Remote System Discovery, Remote Services, Remote Services: Distributed Component Object Model, Obfuscated Files or Information, Obfuscated Files or Information: Command Obfuscation, System Owner/User Discovery, Masquerading, Masquerading: Match Legitimate Name or Location, Exfiltration Over C2 Channel, Network Service Discovery, Windows Management Instrumentation, System Network Connections Discovery, Process Discovery, Command and Scripting Interpreter, Command and Scripting Interpreter: PowerShell, Permission Groups Discovery, Permission Groups Discovery: Domain Groups, System Information Discovery, File and Directory Discovery, Account Discovery, Account Discovery: Domain Account, Web Service, Ingress Tool Transfer, Network Share Discovery, User Execution, User Execution: Malicious File, System Binary Proxy Execution, System Binary Proxy Execution: Mshta, Domain Trust Discovery, Virtualization/Sandbox Evasion, Virtualization/Sandbox Evasion: System Checks, Abuse Elevation Control Mechanism, Abuse Elevation Control Mechanism: Bypass User Account Control, Use Alternate Authentication Material, Use Alternate Authentication Material: Pass the Hash, Credentials from Password Stores, Steal or Forge Kerberos Tickets, Steal or Forge Kerberos Tickets: Kerberoasting, Hide Artifacts, Hide Artifacts: NTFS File Attributes, Obtain Capabilities, Obtain Capabilities: Tool, Group Policy Discovery

Incident Summary

The incident on the XDRI network began on 2025-05-07T10:40:01.000Z and was confirmed by Sam Sanderson on 2025-09-29T11:55:42.805Z. The violation was likely caused by exploitation of remote services and credential theft. The incident was closed on 2025-09-28T10:27:26.246Z. The investigation revealed significant adversary activity across 6 devices and 5 user accounts, including SYSTEM, vic, remi, pat, and krbtgt. Adversaries employed numerous techniques such as [T1003] OS Credential Dumping, [T1021] Remote Services, [T1059.001] Command and Scripting Interpreter: PowerShell, and [T1041] Exfiltration Over C2 Channel, among others, under tactics like [TA0006] Credential Access, [TA0008] Lateral Movement, and [TA0010] Exfiltration. Products used in the analysis included NGFW Event Service, Secure Endpoint, and Microsoft Defender for Endpoint. Errors were noted in Secure Email Threat Defense, specifically a client error related to IPv4 validation. Remediation actions were executed by Cisco Security Workshop - RIR, including modifications to detection sources, tactics, and techniques.

Event Summary

1. user XDRI/vic
   - 2025-05-07T10:40:01.000Z: accessed device Vic indicating **Suspicious Endpoint Activity (XDR Endpoint)**, **Mshta Remote Payload Execution (Cisco Secure Endpoint)**, **Windows User Account Control Disabled In Registry (Cisco Secure Endpoint)**, **Mimikatz Dump Credentials Execution (Cisco Secure Endpoint)**, **PowerShell Exploitation Framework Commandlets (Cisco Secure Endpoint)**, **Mimikatz Dump Credentials (Cisco Secure Endpoint)**, **Command References Remote Red Team Tools (Cisco Secure Endpoint)**, **PowerShell Download String (Cisco Secure Endpoint)**, **Raw GitHub Argument (Cisco Secure Endpoint)**, **PowerShell Exploitation Framework Commandlets (IEX) (Cisco Secure Endpoint)**, **Read Process Memory of LSASS by PowerShell (Cisco Secure Endpoint)**, **PowerView Module Loaded (Cisco Secure Endpoint)**, **Active Directory Enumeration of Unconstrained Delegation (Cisco Secure Endpoint)**
   - 2025-05-07T10:40:01.000Z: assigned to device Vic indicating **Suspicious Endpoint Activity (XDR Endpoint)**, **Mshta Remote Payload Execution (Cisco Secure Endpoint)**, **Windows User Account Control Disabled In Registry (Cisco Secure Endpoint)**, **Mimikatz Dump Credentials Execution (Cisco Secure Endpoint)**, **PowerShell Exploitation Framework Commandlets (Cisco Secure Endpoint)**, **Mimikatz Dump Credentials (Cisco Secure Endpoint)**, **Command References Remote Red Team Tools (Cisco Secure Endpoint)**, **PowerShell Download String (Cisco Secure Endpoint)**, **Raw GitHub Argument (Cisco Secure Endpoint)**, **PowerShell Exploitation Framework Commandlets (IEX) (Cisco Secure Endpoint)**, **Read Process Memory of LSASS by PowerShell (Cisco Secure Endpoint)**, **PowerView Module Loaded (Cisco Secure Endpoint)**, **Active Directory Enumeration of Unconstrained Delegation (Cisco Secure Endpoint)**
   - 2025-09-22T04:02:15.000Z: executed process svchost[.]exe indicating **System file masquerade (Microsoft Defender for Endpoint)**, **Suspicious PowerShell command line (Microsoft Defender for Endpoint)**, **Suspicious Endpoint Activity (XDR Endpoint)**, **System Binary Executed from an Unusual Location - Suspicious Endpoint Activity (Cisco XDR)**, **Malicious Process Detected - Suspicious Endpoint Activity (Cisco XDR)**, **Suspicious Process Discovery (Microsoft Defender for Endpoint)**, **Suspicious process executed PowerShell command (Microsoft Defender for Endpoint)**, **An active 'SandCat' malware process was detected while executing (Microsoft Defender for Endpoint)**, **PowerShell Exploitation Framework Commandlets (Cisco Secure Endpoint)**, **Mimikatz Dump Credentials (Cisco Secure Endpoint)**, **Command References Remote Red Team Tools (Cisco Secure Endpoint)**, **PowerShell Download String (Cisco Secure Endpoint)**, **Raw GitHub Argument (Cisco Secure Endpoint)**, **Possible attempt to steal credentials (Microsoft Defender for Endpoint)**, **Suspicious System Hardware Discovery (Microsoft Defender for Endpoint)**, **Suspicious Network Share Discovery (Microsoft Defender for Endpoint)**, **Suspicious File and Directory Discovery (Microsoft Defender for Endpoint)**,

Process execution from an alternate data stream (ADS) (Microsoft Defender for Endpoint), **Suspicious WMI process creation (Microsoft Defender for Endpoint)**

- 2025-09-22T04:02:19.588Z: executed process powershell[.]exe indicating **System file masquerade (Microsoft Defender for Endpoint)**, **Suspicious PowerShell command line (Microsoft Defender for Endpoint)**, **Suspicious Endpoint Activity (XDR Endpoint)**, **Base64 Encoding Detected - Suspicious Endpoint Activity (Cisco XDR)**, **System Binary Executed from an Unusual Location - Suspicious Endpoint Activity (Cisco XDR)**, **Malicious Process Detected - Suspicious Endpoint Activity (Cisco XDR)**, **Suspicious mshta process launched (Microsoft Defender for Endpoint)**, **Suspicious Process Discovery (Microsoft Defender for Endpoint)**, **Suspicious process executed PowerShell command (Microsoft Defender for Endpoint)**, **An active 'SandCat' malware process was detected while executing (Microsoft Defender for Endpoint)**, **Windows User Account Control Disabled In Registry (Cisco Secure Endpoint)**, **Mimikatz Dump Credentials Execution (Cisco Secure Endpoint)**, **PowerShell Exploitation Framework Commandlets (Cisco Secure Endpoint)**, **Mimikatz Dump Credentials (Cisco Secure Endpoint)**, **Command References Remote Red Team Tools (Cisco Secure Endpoint)**, **PowerShell Download String (Cisco Secure Endpoint)**, **Raw GitHub Argument (Cisco Secure Endpoint)**, **PowerShell Exploitation Framework Commandlets (IEX) (Cisco Secure Endpoint)**, **Read Process Memory of LSASS by PowerShell (Cisco Secure Endpoint)**, **Possible attempt to steal credentials (Microsoft Defender for Endpoint)**, **Suspicious System Hardware Discovery (Microsoft Defender for Endpoint)**, **Suspicious Network Share Discovery (Microsoft Defender for Endpoint)**, **Suspicious File and Directory Discovery (Microsoft Defender for Endpoint)**, **PowerView Module Loaded (Cisco Secure Endpoint)**, **Active Directory Enumeration of Unconstrained Delegation (Cisco Secure Endpoint)**, **Process execution from an alternate data stream (ADS) (Microsoft Defender for Endpoint)**, **Suspicious remote PowerShell execution (Microsoft Defender for Endpoint)**, **A suspicious file was observed (Microsoft Defender for Endpoint)**, **Suspicious WMI activity initiated remotely (Microsoft Defender for Endpoint)**, **Suspicious file from a remote origin launched (Microsoft Defender for Endpoint)**, **Suspicious sequence of exploration activities (Microsoft Defender for Endpoint)**, **Suspicious Use of Discovery Tools - Suspicious Endpoint Activity (Cisco XDR)** (3 times)
- 2025-09-22T04:02:19.588Z: executed process WMIC.exe indicating **Process execution from an alternate data stream (ADS) (Microsoft Defender for Endpoint)**, **Suspicious WMI process creation (Microsoft Defender for Endpoint)**, **A suspicious file was observed (Microsoft Defender for Endpoint)**, **Suspicious WMI activity initiated remotely (Microsoft Defender for Endpoint)**, **Suspicious file from a remote origin launched (Microsoft Defender for Endpoint)**, **Suspicious sequence of exploration activities (Microsoft Defender for Endpoint)**
- 2025-09-22T04:02:19.588Z: executed process netsh[.]exe indicating **A suspicious file was observed (Microsoft Defender for Endpoint)**, **Suspicious WMI activity initiated remotely (Microsoft Defender for Endpoint)**, **Suspicious file from a remote origin launched (Microsoft Defender for Endpoint)**, **Suspicious sequence of exploration activities (Microsoft Defender for Endpoint)**

- 2025-09-22T04:02:19.588Z: executed process powershell[.]exe indicating **System file masquerade (Microsoft Defender for Endpoint)**, **Suspicious PowerShell command line (Microsoft Defender for Endpoint)**, **Suspicious Endpoint Activity (XDR Endpoint)**, **Base64 Encoding Detected - Suspicious Endpoint Activity (Cisco XDR)**, **System Binary Executed from an Unusual Location - Suspicious Endpoint Activity (Cisco XDR)**, **Malicious Process Detected - Suspicious Endpoint Activity (Cisco XDR)**, **Suspicious mshta process launched (Microsoft Defender for Endpoint)**, **Suspicious Process Discovery (Microsoft Defender for Endpoint)**, **Suspicious process executed PowerShell command (Microsoft Defender for Endpoint)**, **An active 'SandCat' malware process was detected while executing (Microsoft Defender for Endpoint)**, **Windows User Account Control Disabled In Registry (Cisco Secure Endpoint)**, **Mimikatz Dump Credentials Execution (Cisco Secure Endpoint)**, **PowerShell Exploitation Framework Commandlets (Cisco Secure Endpoint)**, **Mimikatz Dump Credentials (Cisco Secure Endpoint)**, **Command References Remote Red Team Tools (Cisco Secure Endpoint)**, **PowerShell Download String (Cisco Secure Endpoint)**, **Raw GitHub Argument (Cisco Secure Endpoint)**, **PowerShell Exploitation Framework Commandlets (IEX) (Cisco Secure Endpoint)**, **Read Process Memory of LSASS by PowerShell (Cisco Secure Endpoint)**, **Possible attempt to steal credentials (Microsoft Defender for Endpoint)**, **Suspicious System Hardware Discovery (Microsoft Defender for Endpoint)**, **Suspicious Network Share Discovery (Microsoft Defender for Endpoint)**, **Suspicious File and Directory Discovery (Microsoft Defender for Endpoint)**, **PowerView Module Loaded (Cisco Secure Endpoint)**, **Active Directory Enumeration of Unconstrained Delegation (Cisco Secure Endpoint)**, **Process execution from an alternate data stream (ADS) (Microsoft Defender for Endpoint)**, **Suspicious remote PowerShell execution (Microsoft Defender for Endpoint)**, **A suspicious file was observed (Microsoft Defender for Endpoint)**, **Suspicious WMI activity initiated remotely (Microsoft Defender for Endpoint)**, **Suspicious file from a remote origin launched (Microsoft Defender for Endpoint)**, **Suspicious sequence of exploration activities (Microsoft Defender for Endpoint)**, **Suspicious Use of Discovery Tools - Suspicious Endpoint Activity (Cisco XDR)**
- 2025-09-22T04:02:19.588Z: assigned to device dc01[.]xdri[.]local indicating **Suspicious Endpoint Activity (XDR Endpoint)**, **Mshta Remote Payload Execution (Cisco Secure Endpoint)**, **Windows User Account Control Disabled In Registry (Cisco Secure Endpoint)**, **Mimikatz Dump Credentials Execution (Cisco Secure Endpoint)**, **PowerShell Exploitation Framework Commandlets (Cisco Secure Endpoint)**, **Mimikatz Dump Credentials (Cisco Secure Endpoint)**, **Command References Remote Red Team Tools (Cisco Secure Endpoint)**, **PowerShell Download String (Cisco Secure Endpoint)**, **Raw GitHub Argument (Cisco Secure Endpoint)**, **PowerShell Exploitation Framework Commandlets (IEX) (Cisco Secure Endpoint)**, **Read Process Memory of LSASS by PowerShell (Cisco Secure Endpoint)**, **PowerView Module Loaded (Cisco Secure Endpoint)**, **Active Directory Enumeration of Unconstrained Delegation (Cisco Secure Endpoint)**, **System Binary Executed from an Unusual Location - Suspicious Endpoint Activity (Cisco XDR)**, **Malicious Process Detected - Suspicious Endpoint Activity (Cisco XDR)**, **Suspicious Use of Discovery Tools - Suspicious Endpoint Activity (Cisco XDR)**

- 2025-09-22T04:02:19.588Z: executed process powershell[.]exe indicating **System file masquerade (Microsoft Defender for Endpoint)**, **Suspicious PowerShell command line (Microsoft Defender for Endpoint)**, **Suspicious Endpoint Activity (XDR Endpoint)**, **Base64 Encoding Detected - Suspicious Endpoint Activity (Cisco XDR)**, **System Binary Executed from an Unusual Location - Suspicious Endpoint Activity (Cisco XDR)**, **Malicious Process Detected - Suspicious Endpoint Activity (Cisco XDR)**, **Suspicious mshta process launched (Microsoft Defender for Endpoint)**, **Suspicious Process Discovery (Microsoft Defender for Endpoint)**, **Suspicious process executed PowerShell command (Microsoft Defender for Endpoint)**, **An active 'SandCat' malware process was detected while executing (Microsoft Defender for Endpoint)**, **Windows User Account Control Disabled In Registry (Cisco Secure Endpoint)**, **Mimikatz Dump Credentials Execution (Cisco Secure Endpoint)**, **PowerShell Exploitation Framework Commandlets (Cisco Secure Endpoint)**, **Mimikatz Dump Credentials (Cisco Secure Endpoint)**, **Command References Remote Red Team Tools (Cisco Secure Endpoint)**, **PowerShell Download String (Cisco Secure Endpoint)**, **Raw GitHub Argument (Cisco Secure Endpoint)**, **PowerShell Exploitation Framework Commandlets (IEX) (Cisco Secure Endpoint)**, **Read Process Memory of LSASS by PowerShell (Cisco Secure Endpoint)**, **Possible attempt to steal credentials (Microsoft Defender for Endpoint)**, **Suspicious System Hardware Discovery (Microsoft Defender for Endpoint)**, **Suspicious Network Share Discovery (Microsoft Defender for Endpoint)**, **Suspicious File and Directory Discovery (Microsoft Defender for Endpoint)**, **PowerView Module Loaded (Cisco Secure Endpoint)**, **Active Directory Enumeration of Unconstrained Delegation (Cisco Secure Endpoint)**, **Process execution from an alternate data stream (ADS) (Microsoft Defender for Endpoint)**, **Suspicious remote PowerShell execution (Microsoft Defender for Endpoint)**, **A suspicious file was observed (Microsoft Defender for Endpoint)**, **Suspicious WMI activity initiated remotely (Microsoft Defender for Endpoint)**, **Suspicious file from a remote origin launched (Microsoft Defender for Endpoint)**, **Suspicious sequence of exploration activities (Microsoft Defender for Endpoint)**, **Suspicious Use of Discovery Tools - Suspicious Endpoint Activity (Cisco XDR)**
- 2025-09-22T04:02:19.588Z: executed process ARP.EXE indicating **A suspicious file was observed (Microsoft Defender for Endpoint)**, **Suspicious WMI activity initiated remotely (Microsoft Defender for Endpoint)**, **Suspicious file from a remote origin launched (Microsoft Defender for Endpoint)**, **Suspicious sequence of exploration activities (Microsoft Defender for Endpoint)**
- 2025-09-22T04:02:19.588Z: executed process cmd[.]exe indicating **System file masquerade (Microsoft Defender for Endpoint)**
- 2025-09-22T04:02:19.588Z: executed process wsmprovhost[.]exe indicating **Process execution from an alternate data stream (ADS) (Microsoft Defender for Endpoint)**, **Suspicious WMI process creation (Microsoft Defender for Endpoint)**
- 2025-09-22T04:02:19.588Z: executed process gpresult[.]exe indicating **A suspicious file was observed (Microsoft Defender for Endpoint)**, **Suspicious WMI activity initiated remotely (Microsoft Defender for Endpoint)**, **Suspicious file from a remote origin launched (Microsoft Defender for Endpoint)**, **Suspicious sequence of exploration activities**

(Microsoft Defender for Endpoint)

- 2025-09-22T04:02:19.588Z: executed process mshta[.]exe indicating **System file masquerade (Microsoft Defender for Endpoint)**, **Suspicious PowerShell command line (Microsoft Defender for Endpoint)**, **Suspicious Endpoint Activity (XDR Endpoint)**, **Suspicious File Download Observed on Process Arguments - Suspicious Endpoint Activity (Cisco XDR)**, **Mshta Remote Payload Execution (Cisco Secure Endpoint)**, **Base64 Encoding Detected - Suspicious Endpoint Activity (Cisco XDR)**, **Suspicious mshta process launched (Microsoft Defender for Endpoint)**, **Suspicious Process Discovery (Microsoft Defender for Endpoint)**, **Suspicious process executed PowerShell command (Microsoft Defender for Endpoint)**
- 2025-09-22T04:02:19.588Z: executed process tasklist[.]exe indicating **A suspicious file was observed (Microsoft Defender for Endpoint)**, **Suspicious WMI activity initiated remotely (Microsoft Defender for Endpoint)**, **Suspicious file from a remote origin launched (Microsoft Defender for Endpoint)**, **Suspicious sequence of exploration activities (Microsoft Defender for Endpoint)**
- 2025-09-22T04:02:19.588Z: executed process nbtstat[.]exe indicating **A suspicious file was observed (Microsoft Defender for Endpoint)**, **Suspicious WMI activity initiated remotely (Microsoft Defender for Endpoint)**, **Suspicious file from a remote origin launched (Microsoft Defender for Endpoint)**, **Suspicious sequence of exploration activities (Microsoft Defender for Endpoint)**
- 2025-09-22T04:02:19.588Z: executed process explorer[.]exe indicating **System file masquerade (Microsoft Defender for Endpoint)**

2. device dc01[.]xdri[.]local
   - 2025-05-07T10:40:01.000Z: was communicated with by ip 198[.]18[.]133[.]150 indicating **SID:1:29957:6 (TALOS)**, **Generic.Hacktool.BeEF.1.DE2EBF48 (null)**, **SID:1:15306:22 (TALOS)**, **SID:1:11192:20 (TALOS)**, **System file masquerade (Microsoft Defender for Endpoint)**, **SID:1:25276:10: Multiple products oversized Content-Length memory corruption attempt (TALOS)**, **SID:1:5708:13: web server file upload attempt (TALOS)**, **SID:1:23626:10 (TALOS)**, **SID:1:20619:6 (TALOS)**, **SID:1:38370:3 (TALOS)**, **SID:1:8068:17 (TALOS)**, **SID:1:42231:3: RTF url moniker COM file download attempt (TALOS)**, **SID:1:44416:3 (TALOS)**, **Suspicious PowerShell command line (Microsoft Defender for Endpoint)**, **SID:1:45745:3: CloudMe Sync Client stack buffer overflow attempt (TALOS)**, **Suspicious Endpoint Activity (XDR Endpoint)**, **Suspicious File Download Observed on Process Arguments - Suspicious Endpoint Activity (Cisco XDR)**, **Mshta Remote Payload Execution (Cisco Secure Endpoint)**, **Base64 Encoding Detected - Suspicious Endpoint Activity (Cisco XDR)**, **System Binary Executed from an Unusual Location - Suspicious Endpoint Activity (Cisco XDR)**, **Malicious Process Detected - Suspicious Endpoint Activity (Cisco XDR)**, **Suspicious mshta process launched (Microsoft Defender for Endpoint)**, **Suspicious Process Discovery (Microsoft Defender for Endpoint)**, **Process execution from an alternate data stream (ADS) (Microsoft Defender for Endpoint)**, **Suspicious WMI process creation (Microsoft Defender for Endpoint)**, **Suspicious File and Directory Discovery (Microsoft Defender for Endpoint)**, **Suspicious Network Share Discovery**

(Microsoft Defender for Endpoint), **Suspicious remote PowerShell execution (Microsoft Defender for Endpoint)**, **A suspicious file was observed (Microsoft Defender for Endpoint)**, **Suspicious WMI activity initiated remotely (Microsoft Defender for Endpoint)**, **Suspicious file from a remote origin launched (Microsoft Defender for Endpoint)**, **Suspicious sequence of exploration activities (Microsoft Defender for Endpoint)**, **Suspicious behavior by svchost[.]exe was observed (Microsoft Defender for Endpoint)**, **Alternate Data Stream Execution (Cisco Secure Endpoint)**, **PowerShell Exploitation Framework Commandlets (Cisco Secure Endpoint)**, **PowerShell Download String (Cisco Secure Endpoint)**, **Command References Remote Red Team Tools (Cisco Secure Endpoint)**, **Raw GitHub Argument (Cisco Secure Endpoint)**, **Mimikatz Dump Credentials (Cisco Secure Endpoint)**

- 2025-05-07T10:40:01.000Z: communicated with device Vic indicating **Suspicious Endpoint Activity (XDR Endpoint)**, **Mshta Remote Payload Execution (Cisco Secure Endpoint)**, **Windows User Account Control Disabled In Registry (Cisco Secure Endpoint)**, **Mimikatz Dump Credentials Execution (Cisco Secure Endpoint)**, **PowerShell Exploitation Framework Commandlets (Cisco Secure Endpoint)**, **Mimikatz Dump Credentials (Cisco Secure Endpoint)**, **Command References Remote Red Team Tools (Cisco Secure Endpoint)**, **PowerShell Download String (Cisco Secure Endpoint)**, **Raw GitHub Argument (Cisco Secure Endpoint)**, **PowerShell Exploitation Framework Commandlets (IEX) (Cisco Secure Endpoint)**, **Read Process Memory of LSASS by PowerShell (Cisco Secure Endpoint)**, **PowerView Module Loaded (Cisco Secure Endpoint)**, **Active Directory Enumeration of Unconstrained Delegation (Cisco Secure Endpoint)**
- 2025-05-07T10:40:01.000Z: connected to device Vic indicating **Suspicious Endpoint Activity (XDR Endpoint)**, **Mshta Remote Payload Execution (Cisco Secure Endpoint)**, **Windows User Account Control Disabled In Registry (Cisco Secure Endpoint)**, **Mimikatz Dump Credentials Execution (Cisco Secure Endpoint)**, **PowerShell Exploitation Framework Commandlets (Cisco Secure Endpoint)**, **Mimikatz Dump Credentials (Cisco Secure Endpoint)**, **Command References Remote Red Team Tools (Cisco Secure Endpoint)**, **PowerShell Download String (Cisco Secure Endpoint)**, **Raw GitHub Argument (Cisco Secure Endpoint)**, **PowerShell Exploitation Framework Commandlets (IEX) (Cisco Secure Endpoint)**, **Read Process Memory of LSASS by PowerShell (Cisco Secure Endpoint)**, **PowerView Module Loaded (Cisco Secure Endpoint)**, **Active Directory Enumeration of Unconstrained Delegation (Cisco Secure Endpoint)**
- 2025-05-07T10:40:01.000Z: accessed device Vic indicating **Suspicious Endpoint Activity (XDR Endpoint)**, **Mshta Remote Payload Execution (Cisco Secure Endpoint)**, **Windows User Account Control Disabled In Registry (Cisco Secure Endpoint)**, **Mimikatz Dump Credentials Execution (Cisco Secure Endpoint)**, **PowerShell Exploitation Framework Commandlets (Cisco Secure Endpoint)**, **Mimikatz Dump Credentials (Cisco Secure Endpoint)**, **Command References Remote Red Team Tools (Cisco Secure Endpoint)**, **PowerShell Download String (Cisco Secure Endpoint)**, **Raw GitHub Argument (Cisco Secure Endpoint)**, **PowerShell Exploitation Framework Commandlets (IEX) (Cisco Secure Endpoint)**, **Read Process Memory of LSASS by PowerShell (Cisco Secure Endpoint)**, **PowerView Module Loaded (Cisco Secure Endpoint)**, **Active Directory Enumeration of**

Unconstrained Delegation (Cisco Secure Endpoint)

- 2025-05-07T10:40:01.000Z: connected to ip 198[.]18[.]133[.]150 indicating **SID:1:29957:6 (TALOS)**, **Generic.Hacktool.BeEF.1.DE2EBF48 (null)**, **SID:1:15306:22 (TALOS)**, **SID:1:11192:20 (TALOS)**, **System file masquerade (Microsoft Defender for Endpoint)**, **SID:1:25276:10: Multiple products oversized Content-Length memory corruption attempt (TALOS)**, **SID:1:5708:13: web server file upload attempt (TALOS)**, **SID:1:23626:10 (TALOS)**, **SID:1:20619:6 (TALOS)**, **SID:1:38370:3 (TALOS)**, **SID:1:8068:17 (TALOS)**, **SID:1:42231:3: RTF url moniker COM file download attempt (TALOS)**, **SID:1:44416:3 (TALOS)**, **Suspicious PowerShell command line (Microsoft Defender for Endpoint)**, **SID:1:45745:3: CloudMe Sync Client stack buffer overflow attempt (TALOS)**, **Suspicious Endpoint Activity (XDR Endpoint)**, **Suspicious File Download Observed on Process Arguments - Suspicious Endpoint Activity (Cisco XDR)**, **Mshta Remote Payload Execution (Cisco Secure Endpoint)**, **Base64 Encoding Detected - Suspicious Endpoint Activity (Cisco XDR)**, **System Binary Executed from an Unusual Location - Suspicious Endpoint Activity (Cisco XDR)**, **Malicious Process Detected - Suspicious Endpoint Activity (Cisco XDR)**, **Suspicious mshta process launched (Microsoft Defender for Endpoint)**, **Suspicious Process Discovery (Microsoft Defender for Endpoint)**, **Process execution from an alternate data stream (ADS) (Microsoft Defender for Endpoint)**, **Suspicious WMI process creation (Microsoft Defender for Endpoint)**, **Suspicious File and Directory Discovery (Microsoft Defender for Endpoint)**, **Suspicious Network Share Discovery (Microsoft Defender for Endpoint)**, **Suspicious remote PowerShell execution (Microsoft Defender for Endpoint)**, **A suspicious file was observed (Microsoft Defender for Endpoint)**, **Suspicious WMI activity initiated remotely (Microsoft Defender for Endpoint)**, **Suspicious file from a remote origin launched (Microsoft Defender for Endpoint)**, **Suspicious sequence of exploration activities (Microsoft Defender for Endpoint)**, **Suspicious behavior by svchost[.]exe was observed (Microsoft Defender for Endpoint)**, **Alternate Data Stream Execution (Cisco Secure Endpoint)**, **PowerShell Exploitation Framework Commandlets (Cisco Secure Endpoint)**, **PowerShell Download String (Cisco Secure Endpoint)**, **Command References Remote Red Team Tools (Cisco Secure Endpoint)**, **Raw GitHub Argument (Cisco Secure Endpoint)**, **Mimikatz Dump Credentials (Cisco Secure Endpoint)**
- 2025-05-07T10:40:01.000Z: executed process iexplore[.]exe indicating **Generic.Hacktool.BeEF.1.DE2EBF48 (null)**, **Suspicious PowerShell command line (Microsoft Defender for Endpoint)**, **Mshta Remote Payload Execution (Cisco Secure Endpoint)**, **Suspicious mshta process launched (Microsoft Defender for Endpoint)**, **Suspicious Process Discovery (Microsoft Defender for Endpoint)**
- 2025-09-22T04:02:15.000Z: was connected by process svchost[.]exe indicating **System file masquerade (Microsoft Defender for Endpoint)**, **Suspicious PowerShell command line (Microsoft Defender for Endpoint)**, **Suspicious Endpoint Activity (XDR Endpoint)**, **System Binary Executed from an Unusual Location - Suspicious Endpoint Activity (Cisco XDR)**, **Malicious Process Detected - Suspicious Endpoint Activity (Cisco XDR)**, **Suspicious Process Discovery (Microsoft Defender for Endpoint)**, **Suspicious process executed PowerShell command (Microsoft Defender for Endpoint)**, **An active 'SandCat' malware**

process was detected while executing (Microsoft Defender for Endpoint), PowerShell Exploitation Framework Commandlets (Cisco Secure Endpoint), Mimikatz Dump Credentials (Cisco Secure Endpoint), Command References Remote Red Team Tools (Cisco Secure Endpoint), PowerShell Download String (Cisco Secure Endpoint), Raw GitHub Argument (Cisco Secure Endpoint), Possible attempt to steal credentials (Microsoft Defender for Endpoint), Suspicious System Hardware Discovery (Microsoft Defender for Endpoint), Suspicious Network Share Discovery (Microsoft Defender for Endpoint), Suspicious File and Directory Discovery (Microsoft Defender for Endpoint), Process execution from an alternate data stream (ADS) (Microsoft Defender for Endpoint), Suspicious WMI process creation (Microsoft Defender for Endpoint), Suspicious behavior by svchost[.]exe was observed (Microsoft Defender for Endpoint), Suspicious WMI activity initiated remotely (Microsoft Defender for Endpoint)

- 2025-09-22T04:02:15.000Z: was observed on by process svchost[.]exe indicating **System file masquerade (Microsoft Defender for Endpoint), Suspicious PowerShell command line (Microsoft Defender for Endpoint), Suspicious Endpoint Activity (XDR Endpoint), System Binary Executed from an Unusual Location - Suspicious Endpoint Activity (Cisco XDR), Malicious Process Detected - Suspicious Endpoint Activity (Cisco XDR), Suspicious Process Discovery (Microsoft Defender for Endpoint), Suspicious process executed PowerShell command (Microsoft Defender for Endpoint), An active 'SandCat' malware process was detected while executing (Microsoft Defender for Endpoint), PowerShell Exploitation Framework Commandlets (Cisco Secure Endpoint), Mimikatz Dump Credentials (Cisco Secure Endpoint), Command References Remote Red Team Tools (Cisco Secure Endpoint), PowerShell Download String (Cisco Secure Endpoint), Raw GitHub Argument (Cisco Secure Endpoint), Possible attempt to steal credentials (Microsoft Defender for Endpoint), Suspicious System Hardware Discovery (Microsoft Defender for Endpoint), Suspicious Network Share Discovery (Microsoft Defender for Endpoint), Suspicious File and Directory Discovery (Microsoft Defender for Endpoint), Process execution from an alternate data stream (ADS) (Microsoft Defender for Endpoint), Suspicious WMI process creation (Microsoft Defender for Endpoint), Suspicious behavior by svchost[.]exe was observed (Microsoft Defender for Endpoint), Suspicious WMI activity initiated remotely (Microsoft Defender for Endpoint)**
- 2025-09-22T04:02:15.000Z: executed process svchost[.]exe indicating **System file masquerade (Microsoft Defender for Endpoint), Suspicious PowerShell command line (Microsoft Defender for Endpoint), Suspicious Endpoint Activity (XDR Endpoint), System Binary Executed from an Unusual Location - Suspicious Endpoint Activity (Cisco XDR), Malicious Process Detected - Suspicious Endpoint Activity (Cisco XDR), Suspicious Process Discovery (Microsoft Defender for Endpoint), Suspicious process executed PowerShell command (Microsoft Defender for Endpoint), An active 'SandCat' malware process was detected while executing (Microsoft Defender for Endpoint), PowerShell Exploitation Framework Commandlets (Cisco Secure Endpoint), Mimikatz Dump Credentials (Cisco Secure Endpoint), Command References Remote Red Team Tools (Cisco Secure Endpoint), PowerShell Download String (Cisco Secure Endpoint), Raw**

GitHub Argument (Cisco Secure Endpoint), **Possible attempt to steal credentials (Microsoft Defender for Endpoint)**, **Suspicious System Hardware Discovery (Microsoft Defender for Endpoint)**, **Suspicious Network Share Discovery (Microsoft Defender for Endpoint)**, **Suspicious File and Directory Discovery (Microsoft Defender for Endpoint)**, **Process execution from an alternate data stream (ADS) (Microsoft Defender for Endpoint)**, **Suspicious WMI process creation (Microsoft Defender for Endpoint)**, **Suspicious behavior by svchost[.]exe was observed (Microsoft Defender for Endpoint)**, **Suspicious WMI activity initiated remotely (Microsoft Defender for Endpoint)**

- 2025-09-22T04:02:15.000Z: accessed process svchost[.]exe indicating **System file masquerade (Microsoft Defender for Endpoint)**, **Suspicious PowerShell command line (Microsoft Defender for Endpoint)**, **Suspicious Endpoint Activity (XDR Endpoint)**, **System Binary Executed from an Unusual Location - Suspicious Endpoint Activity (Cisco XDR)**, **Malicious Process Detected - Suspicious Endpoint Activity (Cisco XDR)**, **Suspicious Process Discovery (Microsoft Defender for Endpoint)**, **Suspicious process executed PowerShell command (Microsoft Defender for Endpoint)**, **An active 'SandCat' malware process was detected while executing (Microsoft Defender for Endpoint)**, **PowerShell Exploitation Framework Commandlets (Cisco Secure Endpoint)**, **Mimikatz Dump Credentials (Cisco Secure Endpoint)**, **Command References Remote Red Team Tools (Cisco Secure Endpoint)**, **PowerShell Download String (Cisco Secure Endpoint)**, **Raw GitHub Argument (Cisco Secure Endpoint)**, **Possible attempt to steal credentials (Microsoft Defender for Endpoint)**, **Suspicious System Hardware Discovery (Microsoft Defender for Endpoint)**, **Suspicious Network Share Discovery (Microsoft Defender for Endpoint)**, **Suspicious File and Directory Discovery (Microsoft Defender for Endpoint)**, **Process execution from an alternate data stream (ADS) (Microsoft Defender for Endpoint)**, **Suspicious WMI process creation (Microsoft Defender for Endpoint)**, **Suspicious behavior by svchost[.]exe was observed (Microsoft Defender for Endpoint)**, **Suspicious WMI activity initiated remotely (Microsoft Defender for Endpoint)**
- 2025-09-22T04:02:19.588Z: was communicated with by url hXXp://198[.]18[.]133[.]150:8888/ indicating **SID:1:29957:6 (TALOS)**, **Generic.Hacktool.BeEF.1.DE2EBF48 (null)**, **SID:1:15306:22 (TALOS)**, **SID:1:11192:20 (TALOS)**, **System file masquerade (Microsoft Defender for Endpoint)**, **SID:1:25276:10: Multiple products oversized Content-Length memory corruption attempt (TALOS)**, **SID:1:5708:13: web server file upload attempt (TALOS)**, **SID:1:23626:10 (TALOS)**, **SID:1:20619:6 (TALOS)**, **SID:1:38370:3 (TALOS)**, **SID:1:8068:17 (TALOS)**, **SID:1:42231:3: RTF url moniker COM file download attempt (TALOS)**, **SID:1:44416:3 (TALOS)**, **Suspicious PowerShell command line (Microsoft Defender for Endpoint)**, **SID:1:45745:3: CloudMe Sync Client stack buffer overflow attempt (TALOS)**, **Suspicious Endpoint Activity (XDR Endpoint)**, **Suspicious File Download Observed on Process Arguments - Suspicious Endpoint Activity (Cisco XDR)**, **Mshta Remote Payload Execution (Cisco Secure Endpoint)**, **Base64 Encoding Detected - Suspicious Endpoint Activity (Cisco XDR)**, **System Binary Executed from an Unusual Location - Suspicious Endpoint Activity (Cisco XDR)**, **Malicious Process Detected - Suspicious Endpoint Activity (Cisco XDR)**, **Suspicious mshta process**

launched (Microsoft Defender for Endpoint), **Suspicious Process Discovery (Microsoft Defender for Endpoint)**, **Process execution from an alternate data stream (ADS) (Microsoft Defender for Endpoint)**, **Suspicious WMI process creation (Microsoft Defender for Endpoint)**, **Suspicious File and Directory Discovery (Microsoft Defender for Endpoint)**, **Suspicious Network Share Discovery (Microsoft Defender for Endpoint)**, **Suspicious remote PowerShell execution (Microsoft Defender for Endpoint)**, **A suspicious file was observed (Microsoft Defender for Endpoint)**, **Suspicious WMI activity initiated remotely (Microsoft Defender for Endpoint)**, **Suspicious file from a remote origin launched (Microsoft Defender for Endpoint)**, **Suspicious sequence of exploration activities (Microsoft Defender for Endpoint)**, **Suspicious behavior by svchost[.]exe was observed (Microsoft Defender for Endpoint)**, **Alternate Data Stream Execution (Cisco Secure Endpoint)**, **PowerShell Exploitation Framework Commandlets (Cisco Secure Endpoint)**, **PowerShell Download String (Cisco Secure Endpoint)**, **Command References Remote Red Team Tools (Cisco Secure Endpoint)**, **Raw GitHub Argument (Cisco Secure Endpoint)**, **Mimikatz Dump Credentials (Cisco Secure Endpoint)**

- 2025-09-22T04:02:19.588Z: was used by process mshta[.]exe indicating **System file masquerade (Microsoft Defender for Endpoint)**, **Suspicious PowerShell command line (Microsoft Defender for Endpoint)**, **Suspicious Endpoint Activity (XDR Endpoint)**, **Suspicious File Download Observed on Process Arguments - Suspicious Endpoint Activity (Cisco XDR)**, **Mshta Remote Payload Execution (Cisco Secure Endpoint)**, **Base64 Encoding Detected - Suspicious Endpoint Activity (Cisco XDR)**, **Suspicious mshta process launched (Microsoft Defender for Endpoint)**, **Suspicious Process Discovery (Microsoft Defender for Endpoint)**, **Suspicious process executed PowerShell command (Microsoft Defender for Endpoint)**
- 2025-09-22T04:02:19.588Z: was connected by process powershell[.]exe indicating **System file masquerade (Microsoft Defender for Endpoint)**, **Suspicious PowerShell command line (Microsoft Defender for Endpoint)**, **Suspicious Endpoint Activity (XDR Endpoint)**, **Base64 Encoding Detected - Suspicious Endpoint Activity (Cisco XDR)**, **System Binary Executed from an Unusual Location - Suspicious Endpoint Activity (Cisco XDR)**, **Malicious Process Detected - Suspicious Endpoint Activity (Cisco XDR)**, **Suspicious mshta process launched (Microsoft Defender for Endpoint)**, **Suspicious Process Discovery (Microsoft Defender for Endpoint)**, **Suspicious process executed PowerShell command (Microsoft Defender for Endpoint)**, **An active 'SandCat' malware process was detected while executing (Microsoft Defender for Endpoint)**, **Windows User Account Control Disabled In Registry (Cisco Secure Endpoint)**, **Mimikatz Dump Credentials Execution (Cisco Secure Endpoint)**, **PowerShell Exploitation Framework Commandlets (Cisco Secure Endpoint)**, **Mimikatz Dump Credentials (Cisco Secure Endpoint)**, **Command References Remote Red Team Tools (Cisco Secure Endpoint)**, **PowerShell Download String (Cisco Secure Endpoint)**, **Raw GitHub Argument (Cisco Secure Endpoint)**, **PowerShell Exploitation Framework Commandlets (IEX) (Cisco Secure Endpoint)**, **Read Process Memory of LSASS by PowerShell (Cisco Secure Endpoint)**, **Possible attempt to steal credentials (Microsoft Defender for Endpoint)**, **Suspicious System Hardware Discovery (Microsoft Defender for**

Endpoint), Suspicious Network Share Discovery (Microsoft Defender for Endpoint), Suspicious File and Directory Discovery (Microsoft Defender for Endpoint), PowerView Module Loaded (Cisco Secure Endpoint), Active Directory Enumeration of Unconstrained Delegation (Cisco Secure Endpoint), Process execution from an alternate data stream (ADS) (Microsoft Defender for Endpoint), Suspicious remote PowerShell execution (Microsoft Defender for Endpoint), A suspicious file was observed (Microsoft Defender for Endpoint), Suspicious WMI activity initiated remotely (Microsoft Defender for Endpoint), Suspicious file from a remote origin launched (Microsoft Defender for Endpoint), Suspicious sequence of exploration activities (Microsoft Defender for Endpoint), Suspicious Use of Discovery Tools - Suspicious Endpoint Activity (Cisco XDR), Suspicious behavior by svchost[.]exe was observed (Microsoft Defender for Endpoint)

- 2025-09-22T04:02:19.588Z: was used by process powershell[.]exe indicating **System file masquerade (Microsoft Defender for Endpoint), Suspicious PowerShell command line (Microsoft Defender for Endpoint), Suspicious Endpoint Activity (XDR Endpoint), Base64 Encoding Detected - Suspicious Endpoint Activity (Cisco XDR), System Binary Executed from an Unusual Location - Suspicious Endpoint Activity (Cisco XDR), Malicious Process Detected - Suspicious Endpoint Activity (Cisco XDR), Suspicious mshta process launched (Microsoft Defender for Endpoint), Suspicious Process Discovery (Microsoft Defender for Endpoint), Suspicious process executed PowerShell command (Microsoft Defender for Endpoint), An active 'SandCat' malware process was detected while executing (Microsoft Defender for Endpoint), Windows User Account Control Disabled In Registry (Cisco Secure Endpoint), Mimikatz Dump Credentials Execution (Cisco Secure Endpoint), PowerShell Exploitation Framework Commandlets (Cisco Secure Endpoint), Mimikatz Dump Credentials (Cisco Secure Endpoint), Command References Remote Red Team Tools (Cisco Secure Endpoint), PowerShell Download String (Cisco Secure Endpoint), Raw GitHub Argument (Cisco Secure Endpoint), PowerShell Exploitation Framework Commandlets (IEX) (Cisco Secure Endpoint), Read Process Memory of LSASS by PowerShell (Cisco Secure Endpoint), Possible attempt to steal credentials (Microsoft Defender for Endpoint), Suspicious System Hardware Discovery (Microsoft Defender for Endpoint), Suspicious Network Share Discovery (Microsoft Defender for Endpoint), Suspicious File and Directory Discovery (Microsoft Defender for Endpoint), PowerView Module Loaded (Cisco Secure Endpoint), Active Directory Enumeration of Unconstrained Delegation (Cisco Secure Endpoint), Process execution from an alternate data stream (ADS) (Microsoft Defender for Endpoint), Suspicious remote PowerShell execution (Microsoft Defender for Endpoint), A suspicious file was observed (Microsoft Defender for Endpoint), Suspicious WMI activity initiated remotely (Microsoft Defender for Endpoint), Suspicious file from a remote origin launched (Microsoft Defender for Endpoint), Suspicious sequence of exploration activities (Microsoft Defender for Endpoint), Suspicious Use of Discovery Tools - Suspicious Endpoint Activity (Cisco XDR), Suspicious behavior by svchost[.]exe was observed (Microsoft Defender for Endpoint)** (2 times)
- 2025-09-22T04:02:19.588Z: was observed on by process svchost[.]exe indicating **System file masquerade (Microsoft Defender for Endpoint), Suspicious PowerShell command line**

(Microsoft Defender for Endpoint), **Suspicious Endpoint Activity (XDR Endpoint)**, **System Binary Executed from an Unusual Location - Suspicious Endpoint Activity (Cisco XDR)**, **Malicious Process Detected - Suspicious Endpoint Activity (Cisco XDR)**, **Suspicious Process Discovery (Microsoft Defender for Endpoint)**, **Suspicious process executed PowerShell command (Microsoft Defender for Endpoint)**, **An active 'SandCat' malware process was detected while executing (Microsoft Defender for Endpoint)**, **PowerShell Exploitation Framework Commandlets (Cisco Secure Endpoint)**, **Mimikatz Dump Credentials (Cisco Secure Endpoint)**, **Command References Remote Red Team Tools (Cisco Secure Endpoint)**, **PowerShell Download String (Cisco Secure Endpoint)**, **Raw GitHub Argument (Cisco Secure Endpoint)**, **Possible attempt to steal credentials (Microsoft Defender for Endpoint)**, **Suspicious System Hardware Discovery (Microsoft Defender for Endpoint)**, **Suspicious Network Share Discovery (Microsoft Defender for Endpoint)**, **Suspicious File and Directory Discovery (Microsoft Defender for Endpoint)**, **Process execution from an alternate data stream (ADS) (Microsoft Defender for Endpoint)**, **Suspicious WMI process creation (Microsoft Defender for Endpoint)**, **Suspicious behavior by svchost[.]exe was observed (Microsoft Defender for Endpoint)**, **Suspicious WMI activity initiated remotely (Microsoft Defender for Endpoint)**

- 2025-09-22T04:02:19.588Z: was used by process svchost[.]exe indicating **System file masquerade (Microsoft Defender for Endpoint)**, **Suspicious PowerShell command line (Microsoft Defender for Endpoint)**, **Suspicious Endpoint Activity (XDR Endpoint)**, **System Binary Executed from an Unusual Location - Suspicious Endpoint Activity (Cisco XDR)**, **Malicious Process Detected - Suspicious Endpoint Activity (Cisco XDR)**, **Suspicious Process Discovery (Microsoft Defender for Endpoint)**, **Suspicious process executed PowerShell command (Microsoft Defender for Endpoint)**, **An active 'SandCat' malware process was detected while executing (Microsoft Defender for Endpoint)**, **PowerShell Exploitation Framework Commandlets (Cisco Secure Endpoint)**, **Mimikatz Dump Credentials (Cisco Secure Endpoint)**, **Command References Remote Red Team Tools (Cisco Secure Endpoint)**, **PowerShell Download String (Cisco Secure Endpoint)**, **Raw GitHub Argument (Cisco Secure Endpoint)**, **Possible attempt to steal credentials (Microsoft Defender for Endpoint)**, **Suspicious System Hardware Discovery (Microsoft Defender for Endpoint)**, **Suspicious Network Share Discovery (Microsoft Defender for Endpoint)**, **Suspicious File and Directory Discovery (Microsoft Defender for Endpoint)**, **Process execution from an alternate data stream (ADS) (Microsoft Defender for Endpoint)**, **Suspicious WMI process creation (Microsoft Defender for Endpoint)**, **Suspicious behavior by svchost[.]exe was observed (Microsoft Defender for Endpoint)**, **Suspicious WMI activity initiated remotely (Microsoft Defender for Endpoint)**
- 2025-09-22T04:02:19.588Z: executed process powershell[.]exe indicating **System file masquerade (Microsoft Defender for Endpoint)**, **Suspicious PowerShell command line (Microsoft Defender for Endpoint)**, **Suspicious Endpoint Activity (XDR Endpoint)**, **Base64 Encoding Detected - Suspicious Endpoint Activity (Cisco XDR)**, **System Binary Executed from an Unusual Location - Suspicious Endpoint Activity (Cisco XDR)**, **Malicious Process Detected - Suspicious Endpoint Activity (Cisco XDR)**, **Suspicious mshta process launched**

(Microsoft Defender for Endpoint), **Suspicious Process Discovery (Microsoft Defender for Endpoint)**, **Suspicious process executed PowerShell command (Microsoft Defender for Endpoint)**, **An active 'SandCat' malware process was detected while executing (Microsoft Defender for Endpoint)**, **Windows User Account Control Disabled In Registry (Cisco Secure Endpoint)**, **Mimikatz Dump Credentials Execution (Cisco Secure Endpoint)**, **PowerShell Exploitation Framework Commandlets (Cisco Secure Endpoint)**, **Mimikatz Dump Credentials (Cisco Secure Endpoint)**, **Command References Remote Red Team Tools (Cisco Secure Endpoint)**, **PowerShell Download String (Cisco Secure Endpoint)**, **Raw GitHub Argument (Cisco Secure Endpoint)**, **PowerShell Exploitation Framework Commandlets (IEX) (Cisco Secure Endpoint)**, **Read Process Memory of LSASS by PowerShell (Cisco Secure Endpoint)**, **Possible attempt to steal credentials (Microsoft Defender for Endpoint)**, **Suspicious System Hardware Discovery (Microsoft Defender for Endpoint)**, **Suspicious Network Share Discovery (Microsoft Defender for Endpoint)**, **Suspicious File and Directory Discovery (Microsoft Defender for Endpoint)**, **PowerView Module Loaded (Cisco Secure Endpoint)**, **Active Directory Enumeration of Unconstrained Delegation (Cisco Secure Endpoint)**, **Process execution from an alternate data stream (ADS) (Microsoft Defender for Endpoint)**, **Suspicious remote PowerShell execution (Microsoft Defender for Endpoint)**, **A suspicious file was observed (Microsoft Defender for Endpoint)**, **Suspicious WMI activity initiated remotely (Microsoft Defender for Endpoint)**, **Suspicious file from a remote origin launched (Microsoft Defender for Endpoint)**, **Suspicious sequence of exploration activities (Microsoft Defender for Endpoint)**, **Suspicious Use of Discovery Tools - Suspicious Endpoint Activity (Cisco XDR)**, **Suspicious behavior by svchost[.]exe was observed (Microsoft Defender for Endpoint)** (4 times)

- 2025-09-22T04:02:19.588Z: executed process svchost[.]exe indicating **System file masquerade (Microsoft Defender for Endpoint)**, **Suspicious PowerShell command line (Microsoft Defender for Endpoint)**, **Suspicious Endpoint Activity (XDR Endpoint)**, **System Binary Executed from an Unusual Location - Suspicious Endpoint Activity (Cisco XDR)**, **Malicious Process Detected - Suspicious Endpoint Activity (Cisco XDR)**, **Suspicious Process Discovery (Microsoft Defender for Endpoint)**, **Suspicious process executed PowerShell command (Microsoft Defender for Endpoint)**, **An active 'SandCat' malware process was detected while executing (Microsoft Defender for Endpoint)**, **PowerShell Exploitation Framework Commandlets (Cisco Secure Endpoint)**, **Mimikatz Dump Credentials (Cisco Secure Endpoint)**, **Command References Remote Red Team Tools (Cisco Secure Endpoint)**, **PowerShell Download String (Cisco Secure Endpoint)**, **Raw GitHub Argument (Cisco Secure Endpoint)**, **Possible attempt to steal credentials (Microsoft Defender for Endpoint)**, **Suspicious System Hardware Discovery (Microsoft Defender for Endpoint)**, **Suspicious Network Share Discovery (Microsoft Defender for Endpoint)**, **Suspicious File and Directory Discovery (Microsoft Defender for Endpoint)**, **Process execution from an alternate data stream (ADS) (Microsoft Defender for Endpoint)**, **Suspicious WMI process creation (Microsoft Defender for Endpoint)**, **Suspicious behavior by svchost[.]exe was observed (Microsoft Defender for Endpoint)**, **Suspicious WMI activity initiated remotely (Microsoft Defender for Endpoint)** (2 times)

- 2025-09-22T04:02:19.588Z: executed process mshta[.]exe indicating **System file masquerade (Microsoft Defender for Endpoint)**, **Suspicious PowerShell command line (Microsoft Defender for Endpoint)**, **Suspicious Endpoint Activity (XDR Endpoint)**, **Suspicious File Download Observed on Process Arguments - Suspicious Endpoint Activity (Cisco XDR)**, **Mshta Remote Payload Execution (Cisco Secure Endpoint)**, **Base64 Encoding Detected - Suspicious Endpoint Activity (Cisco XDR)**, **Suspicious mshta process launched (Microsoft Defender for Endpoint)**, **Suspicious Process Discovery (Microsoft Defender for Endpoint)**, **Suspicious process executed PowerShell command (Microsoft Defender for Endpoint)**
- 2025-09-22T04:02:19.588Z: accessed process svchost[.]exe indicating **System file masquerade (Microsoft Defender for Endpoint)**, **Suspicious PowerShell command line (Microsoft Defender for Endpoint)**, **Suspicious Endpoint Activity (XDR Endpoint)**, **System Binary Executed from an Unusual Location - Suspicious Endpoint Activity (Cisco XDR)**, **Malicious Process Detected - Suspicious Endpoint Activity (Cisco XDR)**, **Suspicious Process Discovery (Microsoft Defender for Endpoint)**, **Suspicious process executed PowerShell command (Microsoft Defender for Endpoint)**, **An active 'SandCat' malware process was detected while executing (Microsoft Defender for Endpoint)**, **PowerShell Exploitation Framework Commandlets (Cisco Secure Endpoint)**, **Mimikatz Dump Credentials (Cisco Secure Endpoint)**, **Command References Remote Red Team Tools (Cisco Secure Endpoint)**, **PowerShell Download String (Cisco Secure Endpoint)**, **Raw GitHub Argument (Cisco Secure Endpoint)**, **Possible attempt to steal credentials (Microsoft Defender for Endpoint)**, **Suspicious System Hardware Discovery (Microsoft Defender for Endpoint)**, **Suspicious Network Share Discovery (Microsoft Defender for Endpoint)**, **Suspicious File and Directory Discovery (Microsoft Defender for Endpoint)**, **Process execution from an alternate data stream (ADS) (Microsoft Defender for Endpoint)**, **Suspicious WMI process creation (Microsoft Defender for Endpoint)**, **Suspicious behavior by svchost[.]exe was observed (Microsoft Defender for Endpoint)**, **Suspicious WMI activity initiated remotely (Microsoft Defender for Endpoint)**
- 2025-09-22T04:02:19.588Z: connected to url hXXp://198[.]18[.]133[.]150:8888/ indicating **SID:1:29957:6 (TALOS)**, **Generic.Hacktool.BeEF.1.DE2EBF48 (null)**, **SID:1:15306:22 (TALOS)**, **SID:1:11192:20 (TALOS)**, **System file masquerade (Microsoft Defender for Endpoint)**, **SID:1:25276:10: Multiple products oversized Content-Length memory corruption attempt (TALOS)**, **SID:1:5708:13: web server file upload attempt (TALOS)**, **SID:1:23626:10 (TALOS)**, **SID:1:20619:6 (TALOS)**, **SID:1:38370:3 (TALOS)**, **SID:1:8068:17 (TALOS)**, **SID:1:42231:3: RTF url moniker COM file download attempt (TALOS)**, **SID:1:44416:3 (TALOS)**, **Suspicious PowerShell command line (Microsoft Defender for Endpoint)**, **SID:1:45745:3: CloudMe Sync Client stack buffer overflow attempt (TALOS)**, **Suspicious Endpoint Activity (XDR Endpoint)**, **Suspicious File Download Observed on Process Arguments - Suspicious Endpoint Activity (Cisco XDR)**, **Mshta Remote Payload Execution (Cisco Secure Endpoint)**, **Base64 Encoding Detected - Suspicious Endpoint Activity (Cisco XDR)**, **System Binary Executed from an Unusual Location - Suspicious Endpoint Activity (Cisco XDR)**, **Malicious Process Detected - Suspicious Endpoint Activity**

(Cisco XDR), **Suspicious mshta process launched (Microsoft Defender for Endpoint)**, **Suspicious Process Discovery (Microsoft Defender for Endpoint)**, **Process execution from an alternate data stream (ADS) (Microsoft Defender for Endpoint)**, **Suspicious WMI process creation (Microsoft Defender for Endpoint)**, **Suspicious File and Directory Discovery (Microsoft Defender for Endpoint)**, **Suspicious Network Share Discovery (Microsoft Defender for Endpoint)**, **Suspicious remote PowerShell execution (Microsoft Defender for Endpoint)**, **A suspicious file was observed (Microsoft Defender for Endpoint)**, **Suspicious WMI activity initiated remotely (Microsoft Defender for Endpoint)**, **Suspicious file from a remote origin launched (Microsoft Defender for Endpoint)**, **Suspicious sequence of exploration activities (Microsoft Defender for Endpoint)**, **Suspicious behavior by svchost[.]exe was observed (Microsoft Defender for Endpoint)**, **Alternate Data Stream Execution (Cisco Secure Endpoint)**, **PowerShell Exploitation Framework Commandlets (Cisco Secure Endpoint)**, **PowerShell Download String (Cisco Secure Endpoint)**, **Command References Remote Red Team Tools (Cisco Secure Endpoint)**, **Raw GitHub Argument (Cisco Secure Endpoint)**, **Mimikatz Dump Credentials (Cisco Secure Endpoint)**

- 2025-09-24T09:33:58.183Z: was communicated with by url hXXps://download[.]sysinternals[.]com/files/PSTools[.]zip/ indicating **Suspicious PowerShell command line (Microsoft Defender for Endpoint)**, **A suspicious file was observed (Microsoft Defender for Endpoint)**, **Suspicious WMI activity initiated remotely (Microsoft Defender for Endpoint)**, **Suspicious file from a remote origin launched (Microsoft Defender for Endpoint)**, **Suspicious sequence of exploration activities (Microsoft Defender for Endpoint)**
- 2025-09-24T09:33:58.183Z: connected to url hXXps://download[.]sysinternals[.]com/files/PSTools[.]zip/ indicating **Suspicious PowerShell command line (Microsoft Defender for Endpoint)**, **A suspicious file was observed (Microsoft Defender for Endpoint)**, **Suspicious WMI activity initiated remotely (Microsoft Defender for Endpoint)**, **Suspicious file from a remote origin launched (Microsoft Defender for Endpoint)**, **Suspicious sequence of exploration activities (Microsoft Defender for Endpoint)**
- 2025-09-24T09:39:12.492Z: was communicated with by url hXXps://raw[.]githubusercontent[.]com/PowerShellMafia/PowerSploit/4c7a2016fc7931cd37273c5d8e17b16d959867b3/Exfiltration/Invoke-Mimikatz[.]ps1/ indicating **Suspicious remote PowerShell execution (Microsoft Defender for Endpoint)**, **A suspicious file was observed (Microsoft Defender for Endpoint)**, **Suspicious WMI activity initiated remotely (Microsoft Defender for Endpoint)**, **Suspicious file from a remote origin launched (Microsoft Defender for Endpoint)**, **Suspicious sequence of exploration activities (Microsoft Defender for Endpoint)**, **Suspicious PowerShell command line (Microsoft Defender for Endpoint)**, **Malicious Process Detected - Suspicious Endpoint Activity (Cisco XDR)**
- 2025-09-24T09:39:12.492Z: was connected by process WmiPrvSE.exe indicating **Process execution from an alternate data stream (ADS) (Microsoft Defender for Endpoint)**, **Suspicious File and Directory Discovery (Microsoft Defender for Endpoint)**, **Suspicious Network Share Discovery (Microsoft Defender for Endpoint)**, **Suspicious Process**

Discovery (Microsoft Defender for Endpoint), **Suspicious remote PowerShell execution (Microsoft Defender for Endpoint)**, **A suspicious file was observed (Microsoft Defender for Endpoint)**, **Suspicious WMI activity initiated remotely (Microsoft Defender for Endpoint)**, **Suspicious file from a remote origin launched (Microsoft Defender for Endpoint)**, **Suspicious sequence of exploration activities (Microsoft Defender for Endpoint)**, **Suspicious PowerShell command line (Microsoft Defender for Endpoint)**, **Suspicious behavior by svchost[.]exe was observed (Microsoft Defender for Endpoint)**, **Suspicious Endpoint Activity (XDR Endpoint)**, **Alternate Data Stream Execution (Cisco Secure Endpoint)**

- 2025-09-24T09:39:12.492Z: was observed on by file wifi[.]ps1 indicating **Suspicious WMI activity initiated remotely (Microsoft Defender for Endpoint)**
- 2025-09-24T09:39:12.492Z: was communicated with by ips 192[.]168[.]6[.]10, 192[.]168[.]6[.]12, 198[.]18[.]6[.]5 and 2 more indicating **A suspicious file was observed (Microsoft Defender for Endpoint)**, **Suspicious WMI activity initiated remotely (Microsoft Defender for Endpoint)**, **Suspicious file from a remote origin launched (Microsoft Defender for Endpoint)**, **Suspicious sequence of exploration activities (Microsoft Defender for Endpoint)**, **Suspicious Use of Discovery Tools - Suspicious Endpoint Activity (Cisco XDR)**
- 2025-09-24T09:39:12.492Z: was communicated with by swc device id 405 indicating **Suspicious Endpoint Activity (XDR Endpoint)**, **Mshta Remote Payload Execution (Cisco Secure Endpoint)**, **Windows User Account Control Disabled In Registry (Cisco Secure Endpoint)**, **Mimikatz Dump Credentials Execution (Cisco Secure Endpoint)**, **PowerShell Exploitation Framework Commandlets (Cisco Secure Endpoint)**, **Mimikatz Dump Credentials (Cisco Secure Endpoint)**, **Command References Remote Red Team Tools (Cisco Secure Endpoint)**, **PowerShell Download String (Cisco Secure Endpoint)**, **Raw GitHub Argument (Cisco Secure Endpoint)**, **PowerShell Exploitation Framework Commandlets (IEX) (Cisco Secure Endpoint)**, **Read Process Memory of LSASS by PowerShell (Cisco Secure Endpoint)**, **PowerView Module Loaded (Cisco Secure Endpoint)**, **Active Directory Enumeration of Unconstrained Delegation (Cisco Secure Endpoint)**, **A suspicious file was observed (Microsoft Defender for Endpoint)**, **Suspicious WMI activity initiated remotely (Microsoft Defender for Endpoint)**, **Suspicious file from a remote origin launched (Microsoft Defender for Endpoint)**, **Suspicious sequence of exploration activities (Microsoft Defender for Endpoint)**
- 2025-09-24T09:39:12.492Z: was used by process nslookup[.]exe indicating **Suspicious Use of Discovery Tools - Suspicious Endpoint Activity (Cisco XDR)** (6 times)
- 2025-09-24T09:39:12.492Z: was used by process powershell[.]exe indicating **System file masquerade (Microsoft Defender for Endpoint)**, **Suspicious PowerShell command line (Microsoft Defender for Endpoint)**, **Suspicious Endpoint Activity (XDR Endpoint)**, **Base64 Encoding Detected - Suspicious Endpoint Activity (Cisco XDR)**, **System Binary Executed from an Unusual Location - Suspicious Endpoint Activity (Cisco XDR)**, **Malicious Process Detected - Suspicious Endpoint Activity (Cisco XDR)**, **Suspicious mshta process launched (Microsoft Defender for Endpoint)**, **Suspicious Process Discovery (Microsoft Defender for Endpoint)**, **Suspicious process executed PowerShell command (Microsoft Defender for**

Endpoint), **An active 'SandCat' malware process was detected while executing (Microsoft Defender for Endpoint)**, **Windows User Account Control Disabled In Registry (Cisco Secure Endpoint)**, **Mimikatz Dump Credentials Execution (Cisco Secure Endpoint)**, **PowerShell Exploitation Framework Commandlets (Cisco Secure Endpoint)**, **Mimikatz Dump Credentials (Cisco Secure Endpoint)**, **Command References Remote Red Team Tools (Cisco Secure Endpoint)**, **PowerShell Download String (Cisco Secure Endpoint)**, **Raw GitHub Argument (Cisco Secure Endpoint)**, **PowerShell Exploitation Framework Commandlets (IEX) (Cisco Secure Endpoint)**, **Read Process Memory of LSASS by PowerShell (Cisco Secure Endpoint)**, **Possible attempt to steal credentials (Microsoft Defender for Endpoint)**, **Suspicious System Hardware Discovery (Microsoft Defender for Endpoint)**, **Suspicious Network Share Discovery (Microsoft Defender for Endpoint)**, **Suspicious File and Directory Discovery (Microsoft Defender for Endpoint)**, **PowerView Module Loaded (Cisco Secure Endpoint)**, **Active Directory Enumeration of Unconstrained Delegation (Cisco Secure Endpoint)**, **Process execution from an alternate data stream (ADS) (Microsoft Defender for Endpoint)**, **Suspicious remote PowerShell execution (Microsoft Defender for Endpoint)**, **A suspicious file was observed (Microsoft Defender for Endpoint)**, **Suspicious WMI activity initiated remotely (Microsoft Defender for Endpoint)**, **Suspicious file from a remote origin launched (Microsoft Defender for Endpoint)**, **Suspicious sequence of exploration activities (Microsoft Defender for Endpoint)**, **Suspicious Use of Discovery Tools - Suspicious Endpoint Activity (Cisco XDR)**, **Suspicious behavior by svchost[.]exe was observed (Microsoft Defender for Endpoint)** (2 times)

- 2025-09-24T09:39:12.492Z: connected to ips 192[.]168[.]6[.]10, 192[.]168[.]6[.]12, 198[.]18[.]6[.]5 and 2 more indicating **A suspicious file was observed (Microsoft Defender for Endpoint)**, **Suspicious WMI activity initiated remotely (Microsoft Defender for Endpoint)**, **Suspicious file from a remote origin launched (Microsoft Defender for Endpoint)**, **Suspicious sequence of exploration activities (Microsoft Defender for Endpoint)**, **Suspicious Use of Discovery Tools - Suspicious Endpoint Activity (Cisco XDR)**
- 2025-09-24T09:39:12.492Z: connected to ips 239[.]255[.]255[.]250, 224[.]0[.]0[.]251, 224[.]0[.]0[.]22 and 1 more indicating **Suspicious WMI activity initiated remotely (Microsoft Defender for Endpoint)**
- 2025-09-24T09:39:12.492Z: executed process mshta[.]exe indicating **System file masquerade (Microsoft Defender for Endpoint)**, **Suspicious PowerShell command line (Microsoft Defender for Endpoint)**, **Suspicious Endpoint Activity (XDR Endpoint)**, **Suspicious File Download Observed on Process Arguments - Suspicious Endpoint Activity (Cisco XDR)**, **Mshta Remote Payload Execution (Cisco Secure Endpoint)**, **Base64 Encoding Detected - Suspicious Endpoint Activity (Cisco XDR)**, **Suspicious mshta process launched (Microsoft Defender for Endpoint)**, **Suspicious Process Discovery (Microsoft Defender for Endpoint)**, **Suspicious process executed PowerShell command (Microsoft Defender for Endpoint)**
- 2025-09-24T09:39:12.492Z: executed process WMIC.exe indicating **Process execution from an alternate data stream (ADS) (Microsoft Defender for Endpoint)**, **Suspicious WMI process creation (Microsoft Defender for Endpoint)**, **A suspicious file was observed**

(Microsoft Defender for Endpoint), **Suspicious WMI activity initiated remotely (Microsoft Defender for Endpoint)**, **Suspicious file from a remote origin launched (Microsoft Defender for Endpoint)**, **Suspicious sequence of exploration activities (Microsoft Defender for Endpoint)**

- 2025-09-24T09:39:12.492Z: connected to device dc01[.]xdri[.]local indicating **Suspicious Endpoint Activity (XDR Endpoint)**, **Mshta Remote Payload Execution (Cisco Secure Endpoint)**, **Windows User Account Control Disabled In Registry (Cisco Secure Endpoint)**, **Mimikatz Dump Credentials Execution (Cisco Secure Endpoint)**, **PowerShell Exploitation Framework Commandlets (Cisco Secure Endpoint)**, **Mimikatz Dump Credentials (Cisco Secure Endpoint)**, **Command References Remote Red Team Tools (Cisco Secure Endpoint)**, **PowerShell Download String (Cisco Secure Endpoint)**, **Raw GitHub Argument (Cisco Secure Endpoint)**, **PowerShell Exploitation Framework Commandlets (IEX) (Cisco Secure Endpoint)**, **Read Process Memory of LSASS by PowerShell (Cisco Secure Endpoint)**, **PowerView Module Loaded (Cisco Secure Endpoint)**, **Active Directory Enumeration of Unconstrained Delegation (Cisco Secure Endpoint)**, **System Binary Executed from an Unusual Location - Suspicious Endpoint Activity (Cisco XDR)**, **Malicious Process Detected - Suspicious Endpoint Activity (Cisco XDR)**, **Suspicious Use of Discovery Tools - Suspicious Endpoint Activity (Cisco XDR)**
- 2025-09-24T09:39:12.492Z: executed processes nbtstat[.]exe, netsh[.]exe, tasklist[.]exe and 3 more indicating **A suspicious file was observed (Microsoft Defender for Endpoint)**, **Suspicious WMI activity initiated remotely (Microsoft Defender for Endpoint)**, **Suspicious file from a remote origin launched (Microsoft Defender for Endpoint)**, **Suspicious sequence of exploration activities (Microsoft Defender for Endpoint)**
- 2025-09-24T09:39:12.492Z: executed process WmiPrvSE.exe indicating **Process execution from an alternate data stream (ADS) (Microsoft Defender for Endpoint)**, **Suspicious File and Directory Discovery (Microsoft Defender for Endpoint)**, **Suspicious Network Share Discovery (Microsoft Defender for Endpoint)**, **Suspicious Process Discovery (Microsoft Defender for Endpoint)**, **Suspicious remote PowerShell execution (Microsoft Defender for Endpoint)**, **A suspicious file was observed (Microsoft Defender for Endpoint)**, **Suspicious WMI activity initiated remotely (Microsoft Defender for Endpoint)**, **Suspicious file from a remote origin launched (Microsoft Defender for Endpoint)**, **Suspicious sequence of exploration activities (Microsoft Defender for Endpoint)**, **Suspicious PowerShell command line (Microsoft Defender for Endpoint)**, **Suspicious behavior by svchost[.]exe was observed (Microsoft Defender for Endpoint)**, **Suspicious Endpoint Activity (XDR Endpoint)**, **Alternate Data Stream Execution (Cisco Secure Endpoint)**
- 2025-09-24T09:39:12.492Z: executed process powershell[.]exe indicating **System file masquerade (Microsoft Defender for Endpoint)**, **Suspicious PowerShell command line (Microsoft Defender for Endpoint)**, **Suspicious Endpoint Activity (XDR Endpoint)**, **Base64 Encoding Detected - Suspicious Endpoint Activity (Cisco XDR)**, **System Binary Executed from an Unusual Location - Suspicious Endpoint Activity (Cisco XDR)**, **Malicious Process Detected - Suspicious Endpoint Activity (Cisco XDR)**, **Suspicious mshta process launched (Microsoft Defender for Endpoint)**, **Suspicious Process Discovery (Microsoft Defender for**

Endpoint), **Suspicious process executed PowerShell command (Microsoft Defender for Endpoint)**, **An active 'SandCat' malware process was detected while executing (Microsoft Defender for Endpoint)**, **Windows User Account Control Disabled In Registry (Cisco Secure Endpoint)**, **Mimikatz Dump Credentials Execution (Cisco Secure Endpoint)**, **PowerShell Exploitation Framework Commandlets (Cisco Secure Endpoint)**, **Mimikatz Dump Credentials (Cisco Secure Endpoint)**, **Command References Remote Red Team Tools (Cisco Secure Endpoint)**, **PowerShell Download String (Cisco Secure Endpoint)**, **Raw GitHub Argument (Cisco Secure Endpoint)**, **PowerShell Exploitation Framework Commandlets (IEX) (Cisco Secure Endpoint)**, **Read Process Memory of LSASS by PowerShell (Cisco Secure Endpoint)**, **Possible attempt to steal credentials (Microsoft Defender for Endpoint)**, **Suspicious System Hardware Discovery (Microsoft Defender for Endpoint)**, **Suspicious Network Share Discovery (Microsoft Defender for Endpoint)**, **Suspicious File and Directory Discovery (Microsoft Defender for Endpoint)**, **PowerView Module Loaded (Cisco Secure Endpoint)**, **Active Directory Enumeration of Unconstrained Delegation (Cisco Secure Endpoint)**, **Process execution from an alternate data stream (ADS) (Microsoft Defender for Endpoint)**, **Suspicious remote PowerShell execution (Microsoft Defender for Endpoint)**, **A suspicious file was observed (Microsoft Defender for Endpoint)**, **Suspicious WMI activity initiated remotely (Microsoft Defender for Endpoint)**, **Suspicious file from a remote origin launched (Microsoft Defender for Endpoint)**, **Suspicious sequence of exploration activities (Microsoft Defender for Endpoint)**, **Suspicious Use of Discovery Tools - Suspicious Endpoint Activity (Cisco XDR)**, **Suspicious behavior by svchost[.]exe was observed (Microsoft Defender for Endpoint)** (15 times)

- 2025-09-24T09:39:12.492Z: executed process wsmprovhost[.]exe indicating **Process execution from an alternate data stream (ADS) (Microsoft Defender for Endpoint)**, **Suspicious WMI process creation (Microsoft Defender for Endpoint)**, **Suspicious WMI activity initiated remotely (Microsoft Defender for Endpoint)** (2 times)
- 2025-09-24T09:39:12.492Z: accessed device dc01[.]xdri[.]local indicating **Suspicious Endpoint Activity (XDR Endpoint)**, **Mshta Remote Payload Execution (Cisco Secure Endpoint)**, **Windows User Account Control Disabled In Registry (Cisco Secure Endpoint)**, **Mimikatz Dump Credentials Execution (Cisco Secure Endpoint)**, **PowerShell Exploitation Framework Commandlets (Cisco Secure Endpoint)**, **Mimikatz Dump Credentials (Cisco Secure Endpoint)**, **Command References Remote Red Team Tools (Cisco Secure Endpoint)**, **PowerShell Download String (Cisco Secure Endpoint)**, **Raw GitHub Argument (Cisco Secure Endpoint)**, **PowerShell Exploitation Framework Commandlets (IEX) (Cisco Secure Endpoint)**, **Read Process Memory of LSASS by PowerShell (Cisco Secure Endpoint)**, **PowerView Module Loaded (Cisco Secure Endpoint)**, **Active Directory Enumeration of Unconstrained Delegation (Cisco Secure Endpoint)**, **System Binary Executed from an Unusual Location - Suspicious Endpoint Activity (Cisco XDR)**, **Malicious Process Detected - Suspicious Endpoint Activity (Cisco XDR)**, **Suspicious Use of Discovery Tools - Suspicious Endpoint Activity (Cisco XDR)**
- 2025-09-24T09:39:12.492Z: executed process powershell[.]exe indicating **System file masquerade (Microsoft Defender for Endpoint)**, **Suspicious PowerShell command line**

(Microsoft Defender for Endpoint), **Suspicious Endpoint Activity (XDR Endpoint)**, **Base64 Encoding Detected - Suspicious Endpoint Activity (Cisco XDR)**, **System Binary Executed from an Unusual Location - Suspicious Endpoint Activity (Cisco XDR)**, **Malicious Process Detected - Suspicious Endpoint Activity (Cisco XDR)**, **Suspicious mshta process launched (Microsoft Defender for Endpoint)**, **Suspicious Process Discovery (Microsoft Defender for Endpoint)**, **Suspicious process executed PowerShell command (Microsoft Defender for Endpoint)**, **An active 'SandCat' malware process was detected while executing (Microsoft Defender for Endpoint)**, **Windows User Account Control Disabled In Registry (Cisco Secure Endpoint)**, **Mimikatz Dump Credentials Execution (Cisco Secure Endpoint)**, **PowerShell Exploitation Framework Commandlets (Cisco Secure Endpoint)**, **Mimikatz Dump Credentials (Cisco Secure Endpoint)**, **Command References Remote Red Team Tools (Cisco Secure Endpoint)**, **PowerShell Download String (Cisco Secure Endpoint)**, **Raw GitHub Argument (Cisco Secure Endpoint)**, **PowerShell Exploitation Framework Commandlets (IEX) (Cisco Secure Endpoint)**, **Read Process Memory of LSASS by PowerShell (Cisco Secure Endpoint)**, **Possible attempt to steal credentials (Microsoft Defender for Endpoint)**, **Suspicious System Hardware Discovery (Microsoft Defender for Endpoint)**, **Suspicious Network Share Discovery (Microsoft Defender for Endpoint)**, **Suspicious File and Directory Discovery (Microsoft Defender for Endpoint)**, **PowerView Module Loaded (Cisco Secure Endpoint)**, **Active Directory Enumeration of Unconstrained Delegation (Cisco Secure Endpoint)**, **Process execution from an alternate data stream (ADS) (Microsoft Defender for Endpoint)**, **Suspicious remote PowerShell execution (Microsoft Defender for Endpoint)**, **A suspicious file was observed (Microsoft Defender for Endpoint)**, **Suspicious WMI activity initiated remotely (Microsoft Defender for Endpoint)**, **Suspicious file from a remote origin launched (Microsoft Defender for Endpoint)**, **Suspicious sequence of exploration activities (Microsoft Defender for Endpoint)**, **Suspicious Use of Discovery Tools - Suspicious Endpoint Activity (Cisco XDR)**, **Suspicious behavior by svchost[.]exe was observed (Microsoft Defender for Endpoint)**

- 2025-09-24T09:39:12.492Z: connected to url hXXps://raw[.]githubusercontent[.]com/PowerShellMafia/PowerSploit/4c7a2016fc7931cd37273c5d8e17b16d959867b3/Exfiltration/Invoke-Mimikatz[.]ps1/ indicating **Suspicious remote PowerShell execution (Microsoft Defender for Endpoint)**, **A suspicious file was observed (Microsoft Defender for Endpoint)**, **Suspicious WMI activity initiated remotely (Microsoft Defender for Endpoint)**, **Suspicious file from a remote origin launched (Microsoft Defender for Endpoint)**, **Suspicious sequence of exploration activities (Microsoft Defender for Endpoint)**, **Suspicious PowerShell command line (Microsoft Defender for Endpoint)**, **Malicious Process Detected - Suspicious Endpoint Activity (Cisco XDR)**
- 2025-09-24T09:39:12.492Z: executed process nslookup[.]exe indicating **Suspicious Use of Discovery Tools - Suspicious Endpoint Activity (Cisco XDR)** (6 times)
- 2025-09-24T09:39:12.492Z: executed process wininit[.]exe indicating **Suspicious remote PowerShell execution (Microsoft Defender for Endpoint)**, **A suspicious file was observed (Microsoft Defender for Endpoint)**, **Suspicious WMI activity initiated remotely (Microsoft Defender for Endpoint)**, **Suspicious file from a remote origin launched (Microsoft Defender**

for Endpoint), **Suspicious sequence of exploration activities (Microsoft Defender for Endpoint)**, **Suspicious PowerShell command line (Microsoft Defender for Endpoint)**

- 2025-09-24T09:39:12.492Z: used by user vic indicating **Suspicious Endpoint Activity (XDR Endpoint)**, **Mshta Remote Payload Execution (Cisco Secure Endpoint)**, **Windows User Account Control Disabled In Registry (Cisco Secure Endpoint)**, **Mimikatz Dump Credentials Execution (Cisco Secure Endpoint)**, **PowerShell Exploitation Framework Commandlets (Cisco Secure Endpoint)**, **Mimikatz Dump Credentials (Cisco Secure Endpoint)**, **Command References Remote Red Team Tools (Cisco Secure Endpoint)**, **PowerShell Download String (Cisco Secure Endpoint)**, **Raw GitHub Argument (Cisco Secure Endpoint)**, **PowerShell Exploitation Framework Commandlets (IEX) (Cisco Secure Endpoint)**, **Read Process Memory of LSASS by PowerShell (Cisco Secure Endpoint)**, **PowerView Module Loaded (Cisco Secure Endpoint)**, **Active Directory Enumeration of Unconstrained Delegation (Cisco Secure Endpoint)**
- 2025-09-24T09:39:12.492Z: executed processes powershell[.]exe, conhost[.]exe indicating **System file masquerade (Microsoft Defender for Endpoint)**, **Suspicious PowerShell command line (Microsoft Defender for Endpoint)**, **Suspicious Endpoint Activity (XDR Endpoint)**, **Base64 Encoding Detected - Suspicious Endpoint Activity (Cisco XDR)**, **System Binary Executed from an Unusual Location - Suspicious Endpoint Activity (Cisco XDR)**, **Malicious Process Detected - Suspicious Endpoint Activity (Cisco XDR)**, **Suspicious mshta process launched (Microsoft Defender for Endpoint)**, **Suspicious Process Discovery (Microsoft Defender for Endpoint)**, **Suspicious process executed PowerShell command (Microsoft Defender for Endpoint)**, **An active 'SandCat' malware process was detected while executing (Microsoft Defender for Endpoint)**, **Windows User Account Control Disabled In Registry (Cisco Secure Endpoint)**, **Mimikatz Dump Credentials Execution (Cisco Secure Endpoint)**, **PowerShell Exploitation Framework Commandlets (Cisco Secure Endpoint)**, **Mimikatz Dump Credentials (Cisco Secure Endpoint)**, **Command References Remote Red Team Tools (Cisco Secure Endpoint)**, **PowerShell Download String (Cisco Secure Endpoint)**, **Raw GitHub Argument (Cisco Secure Endpoint)**, **PowerShell Exploitation Framework Commandlets (IEX) (Cisco Secure Endpoint)**, **Read Process Memory of LSASS by PowerShell (Cisco Secure Endpoint)**, **Possible attempt to steal credentials (Microsoft Defender for Endpoint)**, **Suspicious System Hardware Discovery (Microsoft Defender for Endpoint)**, **Suspicious Network Share Discovery (Microsoft Defender for Endpoint)**, **Suspicious File and Directory Discovery (Microsoft Defender for Endpoint)**, **PowerView Module Loaded (Cisco Secure Endpoint)**, **Active Directory Enumeration of Unconstrained Delegation (Cisco Secure Endpoint)**, **Process execution from an alternate data stream (ADS) (Microsoft Defender for Endpoint)**, **Suspicious remote PowerShell execution (Microsoft Defender for Endpoint)**, **A suspicious file was observed (Microsoft Defender for Endpoint)**, **Suspicious WMI activity initiated remotely (Microsoft Defender for Endpoint)**, **Suspicious file from a remote origin launched (Microsoft Defender for Endpoint)**, **Suspicious sequence of exploration activities (Microsoft Defender for Endpoint)**, **Suspicious Use of Discovery Tools - Suspicious Endpoint Activity (Cisco XDR)**, **Suspicious behavior by svchost[.]exe was observed**

(Microsoft Defender for Endpoint)

- 2025-09-24T09:39:12.492Z: connected to ip 192[.]168[.]6[.]135 indicating **A suspicious file was observed (Microsoft Defender for Endpoint)**, **Suspicious WMI activity initiated remotely (Microsoft Defender for Endpoint)**, **Suspicious file from a remote origin launched (Microsoft Defender for Endpoint)**, **Suspicious sequence of exploration activities (Microsoft Defender for Endpoint)**, **Suspicious Use of Discovery Tools - Suspicious Endpoint Activity (Cisco XDR)**
- 2025-09-24T09:39:12.492Z: executed process WmiPrvSE.exe indicating **Process execution from an alternate data stream (ADS) (Microsoft Defender for Endpoint)**, **Suspicious File and Directory Discovery (Microsoft Defender for Endpoint)**, **Suspicious Network Share Discovery (Microsoft Defender for Endpoint)**, **Suspicious Process Discovery (Microsoft Defender for Endpoint)**, **Suspicious remote PowerShell execution (Microsoft Defender for Endpoint)**, **A suspicious file was observed (Microsoft Defender for Endpoint)**, **Suspicious WMI activity initiated remotely (Microsoft Defender for Endpoint)**, **Suspicious file from a remote origin launched (Microsoft Defender for Endpoint)**, **Suspicious sequence of exploration activities (Microsoft Defender for Endpoint)**, **Suspicious PowerShell command line (Microsoft Defender for Endpoint)**, **Suspicious behavior by svchost[.]exe was observed (Microsoft Defender for Endpoint)**, **Suspicious Endpoint Activity (XDR Endpoint)**, **Alternate Data Stream Execution (Cisco Secure Endpoint)** (2 times)
- 2025-09-24T09:39:12.492Z: executed process lsass[.]exe indicating **Suspicious remote PowerShell execution (Microsoft Defender for Endpoint)**, **A suspicious file was observed (Microsoft Defender for Endpoint)**, **Suspicious WMI activity initiated remotely (Microsoft Defender for Endpoint)**, **Suspicious file from a remote origin launched (Microsoft Defender for Endpoint)**, **Suspicious sequence of exploration activities (Microsoft Defender for Endpoint)**, **Suspicious PowerShell command line (Microsoft Defender for Endpoint)**

3. user vic
   - 2025-05-07T10:40:01.000Z: accessed device Vic indicating **Suspicious Endpoint Activity (XDR Endpoint)**, **Mshta Remote Payload Execution (Cisco Secure Endpoint)**, **Windows User Account Control Disabled In Registry (Cisco Secure Endpoint)**, **Mimikatz Dump Credentials Execution (Cisco Secure Endpoint)**, **PowerShell Exploitation Framework Commandlets (Cisco Secure Endpoint)**, **Mimikatz Dump Credentials (Cisco Secure Endpoint)**, **Command References Remote Red Team Tools (Cisco Secure Endpoint)**, **PowerShell Download String (Cisco Secure Endpoint)**, **Raw GitHub Argument (Cisco Secure Endpoint)**, **PowerShell Exploitation Framework Commandlets (IEX) (Cisco Secure Endpoint)**, **Read Process Memory of LSASS by PowerShell (Cisco Secure Endpoint)**, **PowerView Module Loaded (Cisco Secure Endpoint)**, **Active Directory Enumeration of Unconstrained Delegation (Cisco Secure Endpoint)**
   - 2025-05-07T10:40:01.000Z: executed process iexplore[.]exe indicating **Generic.Hacktool.BeEF.1.DE2EBF48 (null)**, **Suspicious PowerShell command line (Microsoft Defender for Endpoint)**, **Mshta Remote Payload Execution (Cisco Secure Endpoint)**, **Suspicious mshta process launched (Microsoft Defender for Endpoint)**, **Suspicious Process Discovery (Microsoft Defender for Endpoint)**

- 2025-09-22T04:02:15.000Z: executed process svchost[.]exe indicating **System file masquerade (Microsoft Defender for Endpoint)**, **Suspicious PowerShell command line (Microsoft Defender for Endpoint)**, **Suspicious Endpoint Activity (XDR Endpoint)**, **System Binary Executed from an Unusual Location - Suspicious Endpoint Activity (Cisco XDR)**, **Malicious Process Detected - Suspicious Endpoint Activity (Cisco XDR)**, **Suspicious Process Discovery (Microsoft Defender for Endpoint)**, **Suspicious process executed PowerShell command (Microsoft Defender for Endpoint)**, **An active 'SandCat' malware process was detected while executing (Microsoft Defender for Endpoint)**, **PowerShell Exploitation Framework Commandlets (Cisco Secure Endpoint)**, **Mimikatz Dump Credentials (Cisco Secure Endpoint)**, **Command References Remote Red Team Tools (Cisco Secure Endpoint)**, **PowerShell Download String (Cisco Secure Endpoint)**, **Raw GitHub Argument (Cisco Secure Endpoint)**, **Possible attempt to steal credentials (Microsoft Defender for Endpoint)**, **Suspicious System Hardware Discovery (Microsoft Defender for Endpoint)**, **Suspicious Network Share Discovery (Microsoft Defender for Endpoint)**, **Suspicious File and Directory Discovery (Microsoft Defender for Endpoint)**, **Process execution from an alternate data stream (ADS) (Microsoft Defender for Endpoint)**, **Suspicious WMI process creation (Microsoft Defender for Endpoint)**
- 2025-09-22T04:02:19.588Z: was used by process svchost[.]exe indicating **System file masquerade (Microsoft Defender for Endpoint)**, **Suspicious PowerShell command line (Microsoft Defender for Endpoint)**, **Suspicious Endpoint Activity (XDR Endpoint)**, **System Binary Executed from an Unusual Location - Suspicious Endpoint Activity (Cisco XDR)**, **Malicious Process Detected - Suspicious Endpoint Activity (Cisco XDR)**, **Suspicious Process Discovery (Microsoft Defender for Endpoint)**, **Suspicious process executed PowerShell command (Microsoft Defender for Endpoint)**, **An active 'SandCat' malware process was detected while executing (Microsoft Defender for Endpoint)**, **PowerShell Exploitation Framework Commandlets (Cisco Secure Endpoint)**, **Mimikatz Dump Credentials (Cisco Secure Endpoint)**, **Command References Remote Red Team Tools (Cisco Secure Endpoint)**, **PowerShell Download String (Cisco Secure Endpoint)**, **Raw GitHub Argument (Cisco Secure Endpoint)**, **Possible attempt to steal credentials (Microsoft Defender for Endpoint)**, **Suspicious System Hardware Discovery (Microsoft Defender for Endpoint)**, **Suspicious Network Share Discovery (Microsoft Defender for Endpoint)**, **Suspicious File and Directory Discovery (Microsoft Defender for Endpoint)**, **Process execution from an alternate data stream (ADS) (Microsoft Defender for Endpoint)**, **Suspicious WMI process creation (Microsoft Defender for Endpoint)**
- 2025-09-22T04:02:19.588Z: was used by process mshta[.]exe indicating **System file masquerade (Microsoft Defender for Endpoint)**, **Suspicious PowerShell command line (Microsoft Defender for Endpoint)**, **Suspicious Endpoint Activity (XDR Endpoint)**, **Suspicious File Download Observed on Process Arguments - Suspicious Endpoint Activity (Cisco XDR)**, **Mshta Remote Payload Execution (Cisco Secure Endpoint)**, **Base64 Encoding Detected - Suspicious Endpoint Activity (Cisco XDR)**, **Suspicious mshta process launched (Microsoft Defender for Endpoint)**, **Suspicious Process Discovery (Microsoft Defender for Endpoint)**, **Suspicious process executed PowerShell command (Microsoft Defender for**

Endpoint)

- 2025-09-22T04:02:19.588Z: was used by process powershell[.]exe indicating **System file masquerade (Microsoft Defender for Endpoint)**, **Suspicious PowerShell command line (Microsoft Defender for Endpoint)**, **Suspicious Endpoint Activity (XDR Endpoint)**, **Base64 Encoding Detected - Suspicious Endpoint Activity (Cisco XDR)**, **System Binary Executed from an Unusual Location - Suspicious Endpoint Activity (Cisco XDR)**, **Malicious Process Detected - Suspicious Endpoint Activity (Cisco XDR)**, **Suspicious mshta process launched (Microsoft Defender for Endpoint)**, **Suspicious Process Discovery (Microsoft Defender for Endpoint)**, **Suspicious process executed PowerShell command (Microsoft Defender for Endpoint)**, **An active 'SandCat' malware process was detected while executing (Microsoft Defender for Endpoint)**, **Windows User Account Control Disabled In Registry (Cisco Secure Endpoint)**, **Mimikatz Dump Credentials Execution (Cisco Secure Endpoint)**, **PowerShell Exploitation Framework Commandlets (Cisco Secure Endpoint)**, **Mimikatz Dump Credentials (Cisco Secure Endpoint)**, **Command References Remote Red Team Tools (Cisco Secure Endpoint)**, **PowerShell Download String (Cisco Secure Endpoint)**, **Raw GitHub Argument (Cisco Secure Endpoint)**, **PowerShell Exploitation Framework Commandlets (IEX) (Cisco Secure Endpoint)**, **Read Process Memory of LSASS by PowerShell (Cisco Secure Endpoint)**, **Possible attempt to steal credentials (Microsoft Defender for Endpoint)**, **Suspicious System Hardware Discovery (Microsoft Defender for Endpoint)**, **Suspicious Network Share Discovery (Microsoft Defender for Endpoint)**, **Suspicious File and Directory Discovery (Microsoft Defender for Endpoint)**, **PowerView Module Loaded (Cisco Secure Endpoint)**, **Active Directory Enumeration of Unconstrained Delegation (Cisco Secure Endpoint)**, **Process execution from an alternate data stream (ADS) (Microsoft Defender for Endpoint)**, **Suspicious remote PowerShell execution (Microsoft Defender for Endpoint)**, **A suspicious file was observed (Microsoft Defender for Endpoint)**, **Suspicious WMI activity initiated remotely (Microsoft Defender for Endpoint)**, **Suspicious file from a remote origin launched (Microsoft Defender for Endpoint)**, **Suspicious sequence of exploration activities (Microsoft Defender for Endpoint)**, **Suspicious Use of Discovery Tools - Suspicious Endpoint Activity (Cisco XDR)** (2 times)
- 2025-09-22T04:02:19.588Z: executed process mshta[.]exe indicating **System file masquerade (Microsoft Defender for Endpoint)**, **Suspicious PowerShell command line (Microsoft Defender for Endpoint)**, **Suspicious Endpoint Activity (XDR Endpoint)**, **Suspicious File Download Observed on Process Arguments - Suspicious Endpoint Activity (Cisco XDR)**, **Mshta Remote Payload Execution (Cisco Secure Endpoint)**, **Base64 Encoding Detected - Suspicious Endpoint Activity (Cisco XDR)**, **Suspicious mshta process launched (Microsoft Defender for Endpoint)**, **Suspicious Process Discovery (Microsoft Defender for Endpoint)**, **Suspicious process executed PowerShell command (Microsoft Defender for Endpoint)**
- 2025-09-22T04:02:19.588Z: executed process powershell[.]exe indicating **System file masquerade (Microsoft Defender for Endpoint)**, **Suspicious PowerShell command line (Microsoft Defender for Endpoint)**, **Suspicious Endpoint Activity (XDR Endpoint)**, **Base64 Encoding Detected - Suspicious Endpoint Activity (Cisco XDR)**, **System Binary Executed**

from an Unusual Location - Suspicious Endpoint Activity (Cisco XDR), **Malicious Process Detected - Suspicious Endpoint Activity (Cisco XDR)**, **Suspicious mshta process launched (Microsoft Defender for Endpoint)**, **Suspicious Process Discovery (Microsoft Defender for Endpoint)**, **Suspicious process executed PowerShell command (Microsoft Defender for Endpoint)**, **An active 'SandCat' malware process was detected while executing (Microsoft Defender for Endpoint)**, **Windows User Account Control Disabled In Registry (Cisco Secure Endpoint)**, **Mimikatz Dump Credentials Execution (Cisco Secure Endpoint)**, **PowerShell Exploitation Framework Commandlets (Cisco Secure Endpoint)**, **Mimikatz Dump Credentials (Cisco Secure Endpoint)**, **Command References Remote Red Team Tools (Cisco Secure Endpoint)**, **PowerShell Download String (Cisco Secure Endpoint)**, **Raw GitHub Argument (Cisco Secure Endpoint)**, **PowerShell Exploitation Framework Commandlets (IEX) (Cisco Secure Endpoint)**, **Read Process Memory of LSASS by PowerShell (Cisco Secure Endpoint)**, **Possible attempt to steal credentials (Microsoft Defender for Endpoint)**, **Suspicious System Hardware Discovery (Microsoft Defender for Endpoint)**, **Suspicious Network Share Discovery (Microsoft Defender for Endpoint)**, **Suspicious File and Directory Discovery (Microsoft Defender for Endpoint)**, **PowerView Module Loaded (Cisco Secure Endpoint)**, **Active Directory Enumeration of Unconstrained Delegation (Cisco Secure Endpoint)**, **Process execution from an alternate data stream (ADS) (Microsoft Defender for Endpoint)**, **Suspicious remote PowerShell execution (Microsoft Defender for Endpoint)**, **A suspicious file was observed (Microsoft Defender for Endpoint)**, **Suspicious WMI activity initiated remotely (Microsoft Defender for Endpoint)**, **Suspicious file from a remote origin launched (Microsoft Defender for Endpoint)**, **Suspicious sequence of exploration activities (Microsoft Defender for Endpoint)**, **Suspicious Use of Discovery Tools - Suspicious Endpoint Activity (Cisco XDR)** (4 times)

- 2025-09-22T04:02:19.588Z: executed process svchost[.]exe indicating **System file masquerade (Microsoft Defender for Endpoint)**, **Suspicious PowerShell command line (Microsoft Defender for Endpoint)**, **Suspicious Endpoint Activity (XDR Endpoint)**, **System Binary Executed from an Unusual Location - Suspicious Endpoint Activity (Cisco XDR)**, **Malicious Process Detected - Suspicious Endpoint Activity (Cisco XDR)**, **Suspicious Process Discovery (Microsoft Defender for Endpoint)**, **Suspicious process executed PowerShell command (Microsoft Defender for Endpoint)**, **An active 'SandCat' malware process was detected while executing (Microsoft Defender for Endpoint)**, **PowerShell Exploitation Framework Commandlets (Cisco Secure Endpoint)**, **Mimikatz Dump Credentials (Cisco Secure Endpoint)**, **Command References Remote Red Team Tools (Cisco Secure Endpoint)**, **PowerShell Download String (Cisco Secure Endpoint)**, **Raw GitHub Argument (Cisco Secure Endpoint)**, **Possible attempt to steal credentials (Microsoft Defender for Endpoint)**, **Suspicious System Hardware Discovery (Microsoft Defender for Endpoint)**, **Suspicious Network Share Discovery (Microsoft Defender for Endpoint)**, **Suspicious File and Directory Discovery (Microsoft Defender for Endpoint)**, **Process execution from an alternate data stream (ADS) (Microsoft Defender for Endpoint)**, **Suspicious WMI process creation (Microsoft Defender for Endpoint)**
- 2025-09-24T09:39:12.492Z: accessed device dc01[.]xdri[.]local indicating **Suspicious**

Endpoint Activity (XDR Endpoint), **Mshta Remote Payload Execution (Cisco Secure Endpoint)**, **Windows User Account Control Disabled In Registry (Cisco Secure Endpoint)**, **Mimikatz Dump Credentials Execution (Cisco Secure Endpoint)**, **PowerShell Exploitation Framework Commandlets (Cisco Secure Endpoint)**, **Mimikatz Dump Credentials (Cisco Secure Endpoint)**, **Command References Remote Red Team Tools (Cisco Secure Endpoint)**, **PowerShell Download String (Cisco Secure Endpoint)**, **Raw GitHub Argument (Cisco Secure Endpoint)**, **PowerShell Exploitation Framework Commandlets (IEX) (Cisco Secure Endpoint)**, **Read Process Memory of LSASS by PowerShell (Cisco Secure Endpoint)**, **PowerView Module Loaded (Cisco Secure Endpoint)**, **Active Directory Enumeration of Unconstrained Delegation (Cisco Secure Endpoint)**, **System Binary Executed from an Unusual Location - Suspicious Endpoint Activity (Cisco XDR)**, **Malicious Process Detected - Suspicious Endpoint Activity (Cisco XDR)**, **Suspicious Use of Discovery Tools - Suspicious Endpoint Activity (Cisco XDR)**

- 2025-09-25T08:52:25.000Z: was used by processes nbtstat[.]exe, netsh[.]exe, tasklist[.]exe and 3 more indicating **A suspicious file was observed (Microsoft Defender for Endpoint)**, **Suspicious WMI activity initiated remotely (Microsoft Defender for Endpoint)**, **Suspicious file from a remote origin launched (Microsoft Defender for Endpoint)**, **Suspicious sequence of exploration activities (Microsoft Defender for Endpoint)**
- 2025-09-25T08:52:25.000Z: was used by process powershell[.]exe indicating **System file masquerade (Microsoft Defender for Endpoint)**, **Suspicious PowerShell command line (Microsoft Defender for Endpoint)**, **Suspicious Endpoint Activity (XDR Endpoint)**, **Base64 Encoding Detected - Suspicious Endpoint Activity (Cisco XDR)**, **System Binary Executed from an Unusual Location - Suspicious Endpoint Activity (Cisco XDR)**, **Malicious Process Detected - Suspicious Endpoint Activity (Cisco XDR)**, **Suspicious mshta process launched (Microsoft Defender for Endpoint)**, **Suspicious Process Discovery (Microsoft Defender for Endpoint)**, **Suspicious process executed PowerShell command (Microsoft Defender for Endpoint)**, **An active 'SandCat' malware process was detected while executing (Microsoft Defender for Endpoint)**, **Windows User Account Control Disabled In Registry (Cisco Secure Endpoint)**, **Mimikatz Dump Credentials Execution (Cisco Secure Endpoint)**, **PowerShell Exploitation Framework Commandlets (Cisco Secure Endpoint)**, **Mimikatz Dump Credentials (Cisco Secure Endpoint)**, **Command References Remote Red Team Tools (Cisco Secure Endpoint)**, **PowerShell Download String (Cisco Secure Endpoint)**, **Raw GitHub Argument (Cisco Secure Endpoint)**, **PowerShell Exploitation Framework Commandlets (IEX) (Cisco Secure Endpoint)**, **Read Process Memory of LSASS by PowerShell (Cisco Secure Endpoint)**, **Possible attempt to steal credentials (Microsoft Defender for Endpoint)**, **Suspicious System Hardware Discovery (Microsoft Defender for Endpoint)**, **Suspicious Network Share Discovery (Microsoft Defender for Endpoint)**, **Suspicious File and Directory Discovery (Microsoft Defender for Endpoint)**, **PowerView Module Loaded (Cisco Secure Endpoint)**, **Active Directory Enumeration of Unconstrained Delegation (Cisco Secure Endpoint)**, **Process execution from an alternate data stream (ADS) (Microsoft Defender for Endpoint)**, **Suspicious remote PowerShell execution (Microsoft Defender for Endpoint)**, **A suspicious file was observed (Microsoft Defender for**

Endpoint), **Suspicious WMI activity initiated remotely (Microsoft Defender for Endpoint)**, **Suspicious file from a remote origin launched (Microsoft Defender for Endpoint)**, **Suspicious sequence of exploration activities (Microsoft Defender for Endpoint)**, **Suspicious Use of Discovery Tools - Suspicious Endpoint Activity (Cisco XDR)** (5 times)

- 2025-09-25T08:52:25.000Z: was used by process nslookup[.]exe indicating **Suspicious Use of Discovery Tools - Suspicious Endpoint Activity (Cisco XDR)** (6 times)
- 2025-09-25T08:52:25.000Z: was used by process wsmprovhost[.]exe indicating **Process execution from an alternate data stream (ADS) (Microsoft Defender for Endpoint)**, **Suspicious WMI process creation (Microsoft Defender for Endpoint)**
- 2025-09-25T08:52:25.000Z: was used by process mshta[.]exe indicating **System file masquerade (Microsoft Defender for Endpoint)**, **Suspicious PowerShell command line (Microsoft Defender for Endpoint)**, **Suspicious Endpoint Activity (XDR Endpoint)**, **Suspicious File Download Observed on Process Arguments - Suspicious Endpoint Activity (Cisco XDR)**, **Mshta Remote Payload Execution (Cisco Secure Endpoint)**, **Base64 Encoding Detected - Suspicious Endpoint Activity (Cisco XDR)**, **Suspicious mshta process launched (Microsoft Defender for Endpoint)**, **Suspicious Process Discovery (Microsoft Defender for Endpoint)**, **Suspicious process executed PowerShell command (Microsoft Defender for Endpoint)**
- 2025-09-25T08:52:25.000Z: was used by process powershell[.]exe indicating **System file masquerade (Microsoft Defender for Endpoint)**, **Suspicious PowerShell command line (Microsoft Defender for Endpoint)**, **Suspicious Endpoint Activity (XDR Endpoint)**, **Base64 Encoding Detected - Suspicious Endpoint Activity (Cisco XDR)**, **System Binary Executed from an Unusual Location - Suspicious Endpoint Activity (Cisco XDR)**, **Malicious Process Detected - Suspicious Endpoint Activity (Cisco XDR)**, **Suspicious mshta process launched (Microsoft Defender for Endpoint)**, **Suspicious Process Discovery (Microsoft Defender for Endpoint)**, **Suspicious process executed PowerShell command (Microsoft Defender for Endpoint)**, **An active 'SandCat' malware process was detected while executing (Microsoft Defender for Endpoint)**, **Windows User Account Control Disabled In Registry (Cisco Secure Endpoint)**, **Mimikatz Dump Credentials Execution (Cisco Secure Endpoint)**, **PowerShell Exploitation Framework Commandlets (Cisco Secure Endpoint)**, **Mimikatz Dump Credentials (Cisco Secure Endpoint)**, **Command References Remote Red Team Tools (Cisco Secure Endpoint)**, **PowerShell Download String (Cisco Secure Endpoint)**, **Raw GitHub Argument (Cisco Secure Endpoint)**, **PowerShell Exploitation Framework Commandlets (IEX) (Cisco Secure Endpoint)**, **Read Process Memory of LSASS by PowerShell (Cisco Secure Endpoint)**, **Possible attempt to steal credentials (Microsoft Defender for Endpoint)**, **Suspicious System Hardware Discovery (Microsoft Defender for Endpoint)**, **Suspicious Network Share Discovery (Microsoft Defender for Endpoint)**, **Suspicious File and Directory Discovery (Microsoft Defender for Endpoint)**, **PowerView Module Loaded (Cisco Secure Endpoint)**, **Active Directory Enumeration of Unconstrained Delegation (Cisco Secure Endpoint)**, **Process execution from an alternate data stream (ADS) (Microsoft Defender for Endpoint)**, **Suspicious remote PowerShell execution (Microsoft Defender for Endpoint)**, **A suspicious file was observed (Microsoft Defender for**

Endpoint), **Suspicious WMI activity initiated remotely (Microsoft Defender for Endpoint)**, **Suspicious file from a remote origin launched (Microsoft Defender for Endpoint)**, **Suspicious sequence of exploration activities (Microsoft Defender for Endpoint)**, **Suspicious Use of Discovery Tools - Suspicious Endpoint Activity (Cisco XDR)**

- 2025-09-25T08:52:25.000Z: was used by processes powershell[.]exe, conhost[.]exe indicating **System file masquerade (Microsoft Defender for Endpoint)**, **Suspicious PowerShell command line (Microsoft Defender for Endpoint)**, **Suspicious Endpoint Activity (XDR Endpoint)**, **Base64 Encoding Detected - Suspicious Endpoint Activity (Cisco XDR)**, **System Binary Executed from an Unusual Location - Suspicious Endpoint Activity (Cisco XDR)**, **Malicious Process Detected - Suspicious Endpoint Activity (Cisco XDR)**, **Suspicious mshta process launched (Microsoft Defender for Endpoint)**, **Suspicious Process Discovery (Microsoft Defender for Endpoint)**, **Suspicious process executed PowerShell command (Microsoft Defender for Endpoint)**, **An active 'SandCat' malware process was detected while executing (Microsoft Defender for Endpoint)**, **Windows User Account Control Disabled In Registry (Cisco Secure Endpoint)**, **Mimikatz Dump Credentials Execution (Cisco Secure Endpoint)**, **PowerShell Exploitation Framework Commandlets (Cisco Secure Endpoint)**, **Mimikatz Dump Credentials (Cisco Secure Endpoint)**, **Command References Remote Red Team Tools (Cisco Secure Endpoint)**, **PowerShell Download String (Cisco Secure Endpoint)**, **Raw GitHub Argument (Cisco Secure Endpoint)**, **PowerShell Exploitation Framework Commandlets (IEX) (Cisco Secure Endpoint)**, **Read Process Memory of LSASS by PowerShell (Cisco Secure Endpoint)**, **Possible attempt to steal credentials (Microsoft Defender for Endpoint)**, **Suspicious System Hardware Discovery (Microsoft Defender for Endpoint)**, **Suspicious Network Share Discovery (Microsoft Defender for Endpoint)**, **Suspicious File and Directory Discovery (Microsoft Defender for Endpoint)**, **PowerView Module Loaded (Cisco Secure Endpoint)**, **Active Directory Enumeration of Unconstrained Delegation (Cisco Secure Endpoint)**, **Process execution from an alternate data stream (ADS) (Microsoft Defender for Endpoint)**, **Suspicious remote PowerShell execution (Microsoft Defender for Endpoint)**, **A suspicious file was observed (Microsoft Defender for Endpoint)**, **Suspicious WMI activity initiated remotely (Microsoft Defender for Endpoint)**, **Suspicious file from a remote origin launched (Microsoft Defender for Endpoint)**, **Suspicious sequence of exploration activities (Microsoft Defender for Endpoint)**, **Suspicious Use of Discovery Tools - Suspicious Endpoint Activity (Cisco XDR)**
- 2025-09-25T08:52:25.000Z: was used by process WMIC.exe indicating **Process execution from an alternate data stream (ADS) (Microsoft Defender for Endpoint)**, **Suspicious WMI process creation (Microsoft Defender for Endpoint)**, **A suspicious file was observed (Microsoft Defender for Endpoint)**, **Suspicious WMI activity initiated remotely (Microsoft Defender for Endpoint)**, **Suspicious file from a remote origin launched (Microsoft Defender for Endpoint)**, **Suspicious sequence of exploration activities (Microsoft Defender for Endpoint)**
- 2025-09-25T08:52:25.000Z: executed processes powershell[.]exe, conhost[.]exe indicating **System file masquerade (Microsoft Defender for Endpoint)**, **Suspicious PowerShell**

command line (Microsoft Defender for Endpoint), **Suspicious Endpoint Activity (XDR Endpoint)**, **Base64 Encoding Detected - Suspicious Endpoint Activity (Cisco XDR)**, **System Binary Executed from an Unusual Location - Suspicious Endpoint Activity (Cisco XDR)**, **Malicious Process Detected - Suspicious Endpoint Activity (Cisco XDR)**, **Suspicious mshta process launched (Microsoft Defender for Endpoint)**, **Suspicious Process Discovery (Microsoft Defender for Endpoint)**, **Suspicious process executed PowerShell command (Microsoft Defender for Endpoint)**, **An active 'SandCat' malware process was detected while executing (Microsoft Defender for Endpoint)**, **Windows User Account Control Disabled In Registry (Cisco Secure Endpoint)**, **Mimikatz Dump Credentials Execution (Cisco Secure Endpoint)**, **PowerShell Exploitation Framework Commandlets (Cisco Secure Endpoint)**, **Mimikatz Dump Credentials (Cisco Secure Endpoint)**, **Command References Remote Red Team Tools (Cisco Secure Endpoint)**, **PowerShell Download String (Cisco Secure Endpoint)**, **Raw GitHub Argument (Cisco Secure Endpoint)**, **PowerShell Exploitation Framework Commandlets (IEX) (Cisco Secure Endpoint)**, **Read Process Memory of LSASS by PowerShell (Cisco Secure Endpoint)**, **Possible attempt to steal credentials (Microsoft Defender for Endpoint)**, **Suspicious System Hardware Discovery (Microsoft Defender for Endpoint)**, **Suspicious Network Share Discovery (Microsoft Defender for Endpoint)**, **Suspicious File and Directory Discovery (Microsoft Defender for Endpoint)**, **PowerView Module Loaded (Cisco Secure Endpoint)**, **Active Directory Enumeration of Unconstrained Delegation (Cisco Secure Endpoint)**, **Process execution from an alternate data stream (ADS) (Microsoft Defender for Endpoint)**, **Suspicious remote PowerShell execution (Microsoft Defender for Endpoint)**, **A suspicious file was observed (Microsoft Defender for Endpoint)**, **Suspicious WMI activity initiated remotely (Microsoft Defender for Endpoint)**, **Suspicious file from a remote origin launched (Microsoft Defender for Endpoint)**, **Suspicious sequence of exploration activities (Microsoft Defender for Endpoint)**, **Suspicious Use of Discovery Tools - Suspicious Endpoint Activity (Cisco XDR)**

- 2025-09-25T08:52:25.000Z: executed process mshta[.]exe indicating **System file masquerade (Microsoft Defender for Endpoint)**, **Suspicious PowerShell command line (Microsoft Defender for Endpoint)**, **Suspicious Endpoint Activity (XDR Endpoint)**, **Suspicious File Download Observed on Process Arguments - Suspicious Endpoint Activity (Cisco XDR)**, **Mshta Remote Payload Execution (Cisco Secure Endpoint)**, **Base64 Encoding Detected - Suspicious Endpoint Activity (Cisco XDR)**, **Suspicious mshta process launched (Microsoft Defender for Endpoint)**, **Suspicious Process Discovery (Microsoft Defender for Endpoint)**, **Suspicious process executed PowerShell command (Microsoft Defender for Endpoint)**
- 2025-09-25T08:52:25.000Z: sent email message Fw: These folks are keen - who is hpurple? - will this ever get through? !!!!
- 2025-09-25T08:52:25.000Z: executed process powershell[.]exe indicating **System file masquerade (Microsoft Defender for Endpoint)**, **Suspicious PowerShell command line (Microsoft Defender for Endpoint)**, **Suspicious Endpoint Activity (XDR Endpoint)**, **Base64 Encoding Detected - Suspicious Endpoint Activity (Cisco XDR)**, **System Binary Executed**

from an Unusual Location - Suspicious Endpoint Activity (Cisco XDR), **Malicious Process Detected - Suspicious Endpoint Activity (Cisco XDR)**, **Suspicious mshta process launched (Microsoft Defender for Endpoint)**, **Suspicious Process Discovery (Microsoft Defender for Endpoint)**, **Suspicious process executed PowerShell command (Microsoft Defender for Endpoint)**, **An active 'SandCat' malware process was detected while executing (Microsoft Defender for Endpoint)**, **Windows User Account Control Disabled In Registry (Cisco Secure Endpoint)**, **Mimikatz Dump Credentials Execution (Cisco Secure Endpoint)**, **PowerShell Exploitation Framework Commandlets (Cisco Secure Endpoint)**, **Mimikatz Dump Credentials (Cisco Secure Endpoint)**, **Command References Remote Red Team Tools (Cisco Secure Endpoint)**, **PowerShell Download String (Cisco Secure Endpoint)**, **Raw GitHub Argument (Cisco Secure Endpoint)**, **PowerShell Exploitation Framework Commandlets (IEX) (Cisco Secure Endpoint)**, **Read Process Memory of LSASS by PowerShell (Cisco Secure Endpoint)**, **Possible attempt to steal credentials (Microsoft Defender for Endpoint)**, **Suspicious System Hardware Discovery (Microsoft Defender for Endpoint)**, **Suspicious Network Share Discovery (Microsoft Defender for Endpoint)**, **Suspicious File and Directory Discovery (Microsoft Defender for Endpoint)**, **PowerView Module Loaded (Cisco Secure Endpoint)**, **Active Directory Enumeration of Unconstrained Delegation (Cisco Secure Endpoint)**, **Process execution from an alternate data stream (ADS) (Microsoft Defender for Endpoint)**, **Suspicious remote PowerShell execution (Microsoft Defender for Endpoint)**, **A suspicious file was observed (Microsoft Defender for Endpoint)**, **Suspicious WMI activity initiated remotely (Microsoft Defender for Endpoint)**, **Suspicious file from a remote origin launched (Microsoft Defender for Endpoint)**, **Suspicious sequence of exploration activities (Microsoft Defender for Endpoint)**, **Suspicious Use of Discovery Tools - Suspicious Endpoint Activity (Cisco XDR)** (14 times)

- 2025-09-25T08:52:25.000Z: executed processes nbtstat[.]exe, netsh[.]exe, tasklist[.]exe and 3 more indicating **A suspicious file was observed (Microsoft Defender for Endpoint)**, **Suspicious WMI activity initiated remotely (Microsoft Defender for Endpoint)**, **Suspicious file from a remote origin launched (Microsoft Defender for Endpoint)**, **Suspicious sequence of exploration activities (Microsoft Defender for Endpoint)**
- 2025-09-25T08:52:25.000Z: executed process wsmprovhost[.]exe indicating **Process execution from an alternate data stream (ADS) (Microsoft Defender for Endpoint)**, **Suspicious WMI process creation (Microsoft Defender for Endpoint)**
- 2025-09-25T08:52:25.000Z: executed process powershell[.]exe indicating **System file masquerade (Microsoft Defender for Endpoint)**, **Suspicious PowerShell command line (Microsoft Defender for Endpoint)**, **Suspicious Endpoint Activity (XDR Endpoint)**, **Base64 Encoding Detected - Suspicious Endpoint Activity (Cisco XDR)**, **System Binary Executed from an Unusual Location - Suspicious Endpoint Activity (Cisco XDR)**, **Malicious Process Detected - Suspicious Endpoint Activity (Cisco XDR)**, **Suspicious mshta process launched (Microsoft Defender for Endpoint)**, **Suspicious Process Discovery (Microsoft Defender for Endpoint)**, **Suspicious process executed PowerShell command (Microsoft Defender for Endpoint)**, **An active 'SandCat' malware process was detected while executing (Microsoft Defender for Endpoint)**, **Windows User Account Control Disabled In Registry (Cisco**

Secure Endpoint), **Mimikatz Dump Credentials Execution (Cisco Secure Endpoint)**, **PowerShell Exploitation Framework Commandlets (Cisco Secure Endpoint)**, **Mimikatz Dump Credentials (Cisco Secure Endpoint)**, **Command References Remote Red Team Tools (Cisco Secure Endpoint)**, **PowerShell Download String (Cisco Secure Endpoint)**, **Raw GitHub Argument (Cisco Secure Endpoint)**, **PowerShell Exploitation Framework Commandlets (IEX) (Cisco Secure Endpoint)**, **Read Process Memory of LSASS by PowerShell (Cisco Secure Endpoint)**, **Possible attempt to steal credentials (Microsoft Defender for Endpoint)**, **Suspicious System Hardware Discovery (Microsoft Defender for Endpoint)**, **Suspicious Network Share Discovery (Microsoft Defender for Endpoint)**, **Suspicious File and Directory Discovery (Microsoft Defender for Endpoint)**, **PowerView Module Loaded (Cisco Secure Endpoint)**, **Active Directory Enumeration of Unconstrained Delegation (Cisco Secure Endpoint)**, **Process execution from an alternate data stream (ADS) (Microsoft Defender for Endpoint)**, **Suspicious remote PowerShell execution (Microsoft Defender for Endpoint)**, **A suspicious file was observed (Microsoft Defender for Endpoint)**, **Suspicious WMI activity initiated remotely (Microsoft Defender for Endpoint)**, **Suspicious file from a remote origin launched (Microsoft Defender for Endpoint)**, **Suspicious sequence of exploration activities (Microsoft Defender for Endpoint)**, **Suspicious Use of Discovery Tools - Suspicious Endpoint Activity (Cisco XDR)**
    - 2025-09-25T08:52:25.000Z: executed process WMIC.exe indicating **Process execution from an alternate data stream (ADS) (Microsoft Defender for Endpoint)**, **Suspicious WMI process creation (Microsoft Defender for Endpoint)**, **A suspicious file was observed (Microsoft Defender for Endpoint)**, **Suspicious WMI activity initiated remotely (Microsoft Defender for Endpoint)**, **Suspicious file from a remote origin launched (Microsoft Defender for Endpoint)**, **Suspicious sequence of exploration activities (Microsoft Defender for Endpoint)**
    - 2025-09-25T08:52:25.000Z: executed process nslookup[.]exe indicating **Suspicious Use of Discovery Tools - Suspicious Endpoint Activity (Cisco XDR)** (6 times)

4. user XDRI/administrator
    - 2025-09-24T09:39:12.492Z: accessed device dc01[.]xdri[.]local
5. user XDRI.LOCAL/vic
    - 2025-09-22T04:02:15.000Z: executed process svchost[.]exe indicating **System file masquerade (Microsoft Defender for Endpoint)**, **Suspicious PowerShell command line (Microsoft Defender for Endpoint)**, **Suspicious Endpoint Activity (XDR Endpoint)**, **System Binary Executed from an Unusual Location - Suspicious Endpoint Activity (Cisco XDR)**, **Malicious Process Detected - Suspicious Endpoint Activity (Cisco XDR)**, **Suspicious Process Discovery (Microsoft Defender for Endpoint)**, **Suspicious process executed PowerShell command (Microsoft Defender for Endpoint)**, **An active 'SandCat' malware process was detected while executing (Microsoft Defender for Endpoint)**, **PowerShell Exploitation Framework Commandlets (Cisco Secure Endpoint)**, **Mimikatz Dump Credentials (Cisco Secure Endpoint)**, **Command References Remote Red Team Tools (Cisco Secure Endpoint)**, **PowerShell Download String (Cisco Secure Endpoint)**, **Raw GitHub Argument (Cisco Secure Endpoint)**, **Possible attempt to steal credentials**

(Microsoft Defender for Endpoint), **Suspicious System Hardware Discovery (Microsoft Defender for Endpoint)**, **Suspicious Network Share Discovery (Microsoft Defender for Endpoint)**, **Suspicious File and Directory Discovery (Microsoft Defender for Endpoint)**, **Process execution from an alternate data stream (ADS) (Microsoft Defender for Endpoint)**, **Suspicious WMI process creation (Microsoft Defender for Endpoint)**

- 2025-09-22T04:02:19.588Z: executed process powershell[.]exe indicating **System file masquerade (Microsoft Defender for Endpoint)**, **Suspicious PowerShell command line (Microsoft Defender for Endpoint)**, **Suspicious Endpoint Activity (XDR Endpoint)**, **Base64 Encoding Detected - Suspicious Endpoint Activity (Cisco XDR)**, **System Binary Executed from an Unusual Location - Suspicious Endpoint Activity (Cisco XDR)**, **Malicious Process Detected - Suspicious Endpoint Activity (Cisco XDR)**, **Suspicious mshta process launched (Microsoft Defender for Endpoint)**, **Suspicious Process Discovery (Microsoft Defender for Endpoint)**, **Suspicious process executed PowerShell command (Microsoft Defender for Endpoint)**, **An active 'SandCat' malware process was detected while executing (Microsoft Defender for Endpoint)**, **Windows User Account Control Disabled In Registry (Cisco Secure Endpoint)**, **Mimikatz Dump Credentials Execution (Cisco Secure Endpoint)**, **PowerShell Exploitation Framework Commandlets (Cisco Secure Endpoint)**, **Mimikatz Dump Credentials (Cisco Secure Endpoint)**, **Command References Remote Red Team Tools (Cisco Secure Endpoint)**, **PowerShell Download String (Cisco Secure Endpoint)**, **Raw GitHub Argument (Cisco Secure Endpoint)**, **PowerShell Exploitation Framework Commandlets (IEX) (Cisco Secure Endpoint)**, **Read Process Memory of LSASS by PowerShell (Cisco Secure Endpoint)**, **Possible attempt to steal credentials (Microsoft Defender for Endpoint)**, **Suspicious System Hardware Discovery (Microsoft Defender for Endpoint)**, **Suspicious Network Share Discovery (Microsoft Defender for Endpoint)**, **Suspicious File and Directory Discovery (Microsoft Defender for Endpoint)**, **PowerView Module Loaded (Cisco Secure Endpoint)**, **Active Directory Enumeration of Unconstrained Delegation (Cisco Secure Endpoint)**, **Process execution from an alternate data stream (ADS) (Microsoft Defender for Endpoint)**, **Suspicious remote PowerShell execution (Microsoft Defender for Endpoint)**, **A suspicious file was observed (Microsoft Defender for Endpoint)**, **Suspicious WMI activity initiated remotely (Microsoft Defender for Endpoint)**, **Suspicious file from a remote origin launched (Microsoft Defender for Endpoint)**, **Suspicious sequence of exploration activities (Microsoft Defender for Endpoint)**, **Suspicious Use of Discovery Tools - Suspicious Endpoint Activity (Cisco XDR)** (5 times)
- 2025-09-24T09:39:12.492Z: executed process ARP.EXE indicating **A suspicious file was observed (Microsoft Defender for Endpoint)**, **Suspicious WMI activity initiated remotely (Microsoft Defender for Endpoint)**, **Suspicious file from a remote origin launched (Microsoft Defender for Endpoint)**, **Suspicious sequence of exploration activities (Microsoft Defender for Endpoint)**
- 2025-09-24T09:39:12.492Z: executed process tasklist[.]exe indicating **A suspicious file was observed (Microsoft Defender for Endpoint)**, **Suspicious WMI activity initiated remotely (Microsoft Defender for Endpoint)**, **Suspicious file from a remote origin launched (Microsoft Defender for Endpoint)**, **Suspicious sequence of exploration activities**

(Microsoft Defender for Endpoint)

- 2025-09-24T09:39:12.492Z: assigned to device dc01[.]xdri[.]local indicating **Suspicious Endpoint Activity (XDR Endpoint)**, **Mshta Remote Payload Execution (Cisco Secure Endpoint)**, **Windows User Account Control Disabled In Registry (Cisco Secure Endpoint)**, **Mimikatz Dump Credentials Execution (Cisco Secure Endpoint)**, **PowerShell Exploitation Framework Commandlets (Cisco Secure Endpoint)**, **Mimikatz Dump Credentials (Cisco Secure Endpoint)**, **Command References Remote Red Team Tools (Cisco Secure Endpoint)**, **PowerShell Download String (Cisco Secure Endpoint)**, **Raw GitHub Argument (Cisco Secure Endpoint)**, **PowerShell Exploitation Framework Commandlets (IEX) (Cisco Secure Endpoint)**, **Read Process Memory of LSASS by PowerShell (Cisco Secure Endpoint)**, **PowerView Module Loaded (Cisco Secure Endpoint)**, **Active Directory Enumeration of Unconstrained Delegation (Cisco Secure Endpoint)**, **System Binary Executed from an Unusual Location - Suspicious Endpoint Activity (Cisco XDR)**, **Malicious Process Detected - Suspicious Endpoint Activity (Cisco XDR)**, **Suspicious Use of Discovery Tools - Suspicious Endpoint Activity (Cisco XDR)**
- 2025-09-24T09:39:12.492Z: executed process gpresult[.]exe indicating **A suspicious file was observed (Microsoft Defender for Endpoint)**, **Suspicious WMI activity initiated remotely (Microsoft Defender for Endpoint)**, **Suspicious file from a remote origin launched (Microsoft Defender for Endpoint)**, **Suspicious sequence of exploration activities (Microsoft Defender for Endpoint)**
- 2025-09-24T09:39:12.492Z: executed process WMIC.exe indicating **Process execution from an alternate data stream (ADS) (Microsoft Defender for Endpoint)**, **Suspicious WMI process creation (Microsoft Defender for Endpoint)**, **A suspicious file was observed (Microsoft Defender for Endpoint)**, **Suspicious WMI activity initiated remotely (Microsoft Defender for Endpoint)**, **Suspicious file from a remote origin launched (Microsoft Defender for Endpoint)**, **Suspicious sequence of exploration activities (Microsoft Defender for Endpoint)**
- 2025-09-24T09:39:12.492Z: executed process nbtstat[.]exe indicating **A suspicious file was observed (Microsoft Defender for Endpoint)**, **Suspicious WMI activity initiated remotely (Microsoft Defender for Endpoint)**, **Suspicious file from a remote origin launched (Microsoft Defender for Endpoint)**, **Suspicious sequence of exploration activities (Microsoft Defender for Endpoint)**
- 2025-09-24T09:39:12.492Z: executed process netsh[.]exe indicating **A suspicious file was observed (Microsoft Defender for Endpoint)**, **Suspicious WMI activity initiated remotely (Microsoft Defender for Endpoint)**, **Suspicious file from a remote origin launched (Microsoft Defender for Endpoint)**, **Suspicious sequence of exploration activities (Microsoft Defender for Endpoint)**

6. device Vic

- 2025-05-07T10:40:01.000Z: was observed on by process svchost[.]exe indicating **System file masquerade (Microsoft Defender for Endpoint)**, **Suspicious PowerShell command line (Microsoft Defender for Endpoint)**, **Suspicious Endpoint Activity (XDR Endpoint)**, **System Binary Executed from an Unusual Location - Suspicious Endpoint Activity (Cisco XDR)**,

Malicious Process Detected - Suspicious Endpoint Activity (Cisco XDR), **Suspicious Process Discovery (Microsoft Defender for Endpoint)**, **Suspicious process executed PowerShell command (Microsoft Defender for Endpoint)**, **An active 'SandCat' malware process was detected while executing (Microsoft Defender for Endpoint)**, **PowerShell Exploitation Framework Commandlets (Cisco Secure Endpoint)**, **Mimikatz Dump Credentials (Cisco Secure Endpoint)**, **Command References Remote Red Team Tools (Cisco Secure Endpoint)**, **PowerShell Download String (Cisco Secure Endpoint)**, **Raw GitHub Argument (Cisco Secure Endpoint)**, **Possible attempt to steal credentials (Microsoft Defender for Endpoint)**, **Suspicious System Hardware Discovery (Microsoft Defender for Endpoint)**, **Suspicious Network Share Discovery (Microsoft Defender for Endpoint)**, **Suspicious File and Directory Discovery (Microsoft Defender for Endpoint)**, **Process execution from an alternate data stream (ADS) (Microsoft Defender for Endpoint)**, **Suspicious WMI process creation (Microsoft Defender for Endpoint)**

- 2025-05-07T10:40:01.000Z: was communicated with by ip 198[.]18[.]133[.]150 indicating **SID:1:29957:6 (TALOS)**, **Generic.Hacktool.BeEF.1.DE2EBF48 (null)**, **SID:1:15306:22 (TALOS)**, **SID:1:11192:20 (TALOS)**, **System file masquerade (Microsoft Defender for Endpoint)**, **SID:1:25276:10: Multiple products oversized Content-Length memory corruption attempt (TALOS)**, **SID:1:5708:13: web server file upload attempt (TALOS)**, **SID:1:23626:10 (TALOS)**, **SID:1:20619:6 (TALOS)**, **SID:1:38370:3 (TALOS)**, **SID:1:8068:17 (TALOS)**, **SID:1:42231:3: RTF url moniker COM file download attempt (TALOS)**, **SID:1:44416:3 (TALOS)**, **Suspicious PowerShell command line (Microsoft Defender for Endpoint)**, **SID:1:45745:3: CloudMe Sync Client stack buffer overflow attempt (TALOS)**, **Suspicious Endpoint Activity (XDR Endpoint)**, **Suspicious File Download Observed on Process Arguments - Suspicious Endpoint Activity (Cisco XDR)**, **Mshta Remote Payload Execution (Cisco Secure Endpoint)**, **Base64 Encoding Detected - Suspicious Endpoint Activity (Cisco XDR)**, **System Binary Executed from an Unusual Location - Suspicious Endpoint Activity (Cisco XDR)**, **Malicious Process Detected - Suspicious Endpoint Activity (Cisco XDR)**, **Suspicious mshta process launched (Microsoft Defender for Endpoint)**, **Suspicious Process Discovery (Microsoft Defender for Endpoint)**, **Process execution from an alternate data stream (ADS) (Microsoft Defender for Endpoint)**, **Suspicious WMI process creation (Microsoft Defender for Endpoint)**, **Suspicious File and Directory Discovery (Microsoft Defender for Endpoint)**, **Suspicious Network Share Discovery (Microsoft Defender for Endpoint)**, **Suspicious remote PowerShell execution (Microsoft Defender for Endpoint)**, **A suspicious file was observed (Microsoft Defender for Endpoint)**, **Suspicious WMI activity initiated remotely (Microsoft Defender for Endpoint)**, **Suspicious file from a remote origin launched (Microsoft Defender for Endpoint)**, **Suspicious sequence of exploration activities (Microsoft Defender for Endpoint)**
- 2025-05-07T10:40:01.000Z: was observed on by process svchost[.]exe indicating **System file masquerade (Microsoft Defender for Endpoint)**, **Suspicious PowerShell command line (Microsoft Defender for Endpoint)**, **Suspicious Endpoint Activity (XDR Endpoint)**, **System Binary Executed from an Unusual Location - Suspicious Endpoint Activity (Cisco XDR)**, **Malicious Process Detected - Suspicious Endpoint Activity (Cisco XDR)**, **Suspicious**

Process Discovery (Microsoft Defender for Endpoint), **Suspicious process executed PowerShell command (Microsoft Defender for Endpoint)**, **An active 'SandCat' malware process was detected while executing (Microsoft Defender for Endpoint)**, **PowerShell Exploitation Framework Commandlets (Cisco Secure Endpoint)**, **Mimikatz Dump Credentials (Cisco Secure Endpoint)**, **Command References Remote Red Team Tools (Cisco Secure Endpoint)**, **PowerShell Download String (Cisco Secure Endpoint)**, **Raw GitHub Argument (Cisco Secure Endpoint)**, **Possible attempt to steal credentials (Microsoft Defender for Endpoint)**, **Suspicious System Hardware Discovery (Microsoft Defender for Endpoint)**, **Suspicious Network Share Discovery (Microsoft Defender for Endpoint)**, **Suspicious File and Directory Discovery (Microsoft Defender for Endpoint)**, **Process execution from an alternate data stream (ADS) (Microsoft Defender for Endpoint)**, **Suspicious WMI process creation (Microsoft Defender for Endpoint)** (3 times)

- 2025-05-07T10:40:01.000Z: was communicated with by hostname attacker[.]ihatemikesimone[.]com indicating **Suspicious Endpoint Activity (XDR Endpoint)**, **Suspicious File Download Observed on Process Arguments - Suspicious Endpoint Activity (Cisco XDR)**, **Base64 Encoding Detected - Suspicious Endpoint Activity (Cisco XDR)**, **System Binary Executed from an Unusual Location - Suspicious Endpoint Activity (Cisco XDR)**, **Malicious Process Detected - Suspicious Endpoint Activity (Cisco XDR)**, **System file masquerade (Microsoft Defender for Endpoint)**, **Suspicious Process Discovery (Microsoft Defender for Endpoint)**, **An active 'SandCat' malware process was detected while executing (Microsoft Defender for Endpoint)**, **PowerShell Exploitation Framework Commandlets (Cisco Secure Endpoint)**, **Mimikatz Dump Credentials (Cisco Secure Endpoint)**, **Command References Remote Red Team Tools (Cisco Secure Endpoint)**, **PowerShell Download String (Cisco Secure Endpoint)**, **Raw GitHub Argument (Cisco Secure Endpoint)**, **Suspicious PowerShell command line (Microsoft Defender for Endpoint)**, **Suspicious Network Share Discovery (Microsoft Defender for Endpoint)**, **Suspicious File and Directory Discovery (Microsoft Defender for Endpoint)**, **Suspicious remote PowerShell execution (Microsoft Defender for Endpoint)**, **A suspicious file was observed (Microsoft Defender for Endpoint)**, **Suspicious WMI activity initiated remotely (Microsoft Defender for Endpoint)**, **Suspicious file from a remote origin launched (Microsoft Defender for Endpoint)**, **Suspicious sequence of exploration activities (Microsoft Defender for Endpoint)**
- 2025-05-07T10:40:01.000Z: was connected by process iexplore[.]exe indicating **Generic.Hacktool.BeEF.1.DE2EBF48 (null)**, **Suspicious PowerShell command line (Microsoft Defender for Endpoint)**, **Mshta Remote Payload Execution (Cisco Secure Endpoint)**, **Suspicious mshta process launched (Microsoft Defender for Endpoint)**, **Suspicious Process Discovery (Microsoft Defender for Endpoint)**
- 2025-05-07T10:40:01.000Z: was communicated with by ip 185[.]199[.]109[.]133 indicating **Malicious Process Detected - Suspicious Endpoint Activity (Cisco XDR)**
- 2025-05-07T10:40:01.000Z: was communicated with by url hXXp://attacker[.]ihatemikesimone[.]com:8888/ indicating **Suspicious Endpoint Activity (XDR Endpoint)**, **Suspicious File Download Observed on Process Arguments - Suspicious**

Endpoint Activity (Cisco XDR), **Base64 Encoding Detected - Suspicious Endpoint Activity (Cisco XDR)**, **System Binary Executed from an Unusual Location - Suspicious Endpoint Activity (Cisco XDR)**, **Malicious Process Detected - Suspicious Endpoint Activity (Cisco XDR)**, **System file masquerade (Microsoft Defender for Endpoint)**, **Suspicious Process Discovery (Microsoft Defender for Endpoint)**, **An active 'SandCat' malware process was detected while executing (Microsoft Defender for Endpoint)**, **PowerShell Exploitation Framework Commandlets (Cisco Secure Endpoint)**, **Mimikatz Dump Credentials (Cisco Secure Endpoint)**, **Command References Remote Red Team Tools (Cisco Secure Endpoint)**, **PowerShell Download String (Cisco Secure Endpoint)**, **Raw GitHub Argument (Cisco Secure Endpoint)**, **Suspicious PowerShell command line (Microsoft Defender for Endpoint)**, **Suspicious Network Share Discovery (Microsoft Defender for Endpoint)**, **Suspicious File and Directory Discovery (Microsoft Defender for Endpoint)**, **Suspicious remote PowerShell execution (Microsoft Defender for Endpoint)**, **A suspicious file was observed (Microsoft Defender for Endpoint)**, **Suspicious WMI activity initiated remotely (Microsoft Defender for Endpoint)**, **Suspicious file from a remote origin launched (Microsoft Defender for Endpoint)**, **Suspicious sequence of exploration activities (Microsoft Defender for Endpoint)**

- 2025-05-07T10:40:01.000Z: was connected by process svchost[.]exe indicating **System file masquerade (Microsoft Defender for Endpoint)**, **Suspicious PowerShell command line (Microsoft Defender for Endpoint)**, **Suspicious Endpoint Activity (XDR Endpoint)**, **System Binary Executed from an Unusual Location - Suspicious Endpoint Activity (Cisco XDR)**, **Malicious Process Detected - Suspicious Endpoint Activity (Cisco XDR)**, **Suspicious Process Discovery (Microsoft Defender for Endpoint)**, **Suspicious process executed PowerShell command (Microsoft Defender for Endpoint)**, **An active 'SandCat' malware process was detected while executing (Microsoft Defender for Endpoint)**, **PowerShell Exploitation Framework Commandlets (Cisco Secure Endpoint)**, **Mimikatz Dump Credentials (Cisco Secure Endpoint)**, **Command References Remote Red Team Tools (Cisco Secure Endpoint)**, **PowerShell Download String (Cisco Secure Endpoint)**, **Raw GitHub Argument (Cisco Secure Endpoint)**, **Possible attempt to steal credentials (Microsoft Defender for Endpoint)**, **Suspicious System Hardware Discovery (Microsoft Defender for Endpoint)**, **Suspicious Network Share Discovery (Microsoft Defender for Endpoint)**, **Suspicious File and Directory Discovery (Microsoft Defender for Endpoint)**, **Process execution from an alternate data stream (ADS) (Microsoft Defender for Endpoint)**, **Suspicious WMI process creation (Microsoft Defender for Endpoint)**
- 2025-05-07T10:40:01.000Z: was connected by process mshta[.]exe indicating **System file masquerade (Microsoft Defender for Endpoint)**, **Suspicious PowerShell command line (Microsoft Defender for Endpoint)**, **Suspicious Endpoint Activity (XDR Endpoint)**, **Suspicious File Download Observed on Process Arguments - Suspicious Endpoint Activity (Cisco XDR)**, **Mshta Remote Payload Execution (Cisco Secure Endpoint)**, **Base64 Encoding Detected - Suspicious Endpoint Activity (Cisco XDR)**, **Suspicious mshta process launched (Microsoft Defender for Endpoint)**, **Suspicious Process Discovery (Microsoft Defender for Endpoint)**, **Suspicious process executed PowerShell command (Microsoft Defender for**

Endpoint)

- 2025-05-07T10:40:01.000Z: was communicated with by ip 198[.]19[.]255[.]146 indicating **System file masquerade (Microsoft Defender for Endpoint)**, **Suspicious PowerShell command line (Microsoft Defender for Endpoint)**, **Suspicious mshta process launched (Microsoft Defender for Endpoint)**, **Suspicious Process Discovery (Microsoft Defender for Endpoint)**, **Suspicious process executed PowerShell command (Microsoft Defender for Endpoint)**, **An active 'SandCat' malware process was detected while executing (Microsoft Defender for Endpoint)**, **Suspicious Network Share Discovery (Microsoft Defender for Endpoint)**, **Suspicious File and Directory Discovery (Microsoft Defender for Endpoint)**
- 2025-05-07T10:40:01.000Z: was connected to ip 198[.]18[.]133[.]150 indicating **SID:1:29957:6 (TALOS)**, **Generic.Hacktool.BeEF.1.DE2EBF48 (null)**, **SID:1:15306:22 (TALOS)**, **SID:1:11192:20 (TALOS)**, **System file masquerade (Microsoft Defender for Endpoint)**, **SID:1:25276:10: Multiple products oversized Content-Length memory corruption attempt (TALOS)**, **SID:1:5708:13: web server file upload attempt (TALOS)**, **SID:1:23626:10 (TALOS)**, **SID:1:20619:6 (TALOS)**, **SID:1:38370:3 (TALOS)**, **SID:1:8068:17 (TALOS)**, **SID:1:42231:3: RTF url moniker COM file download attempt (TALOS)**, **SID:1:44416:3 (TALOS)**, **Suspicious PowerShell command line (Microsoft Defender for Endpoint)**, **SID:1:45745:3: CloudMe Sync Client stack buffer overflow attempt (TALOS)**, **Suspicious Endpoint Activity (XDR Endpoint)**, **Suspicious File Download Observed on Process Arguments - Suspicious Endpoint Activity (Cisco XDR)**, **Mshta Remote Payload Execution (Cisco Secure Endpoint)**, **Base64 Encoding Detected - Suspicious Endpoint Activity (Cisco XDR)**, **System Binary Executed from an Unusual Location - Suspicious Endpoint Activity (Cisco XDR)**, **Malicious Process Detected - Suspicious Endpoint Activity (Cisco XDR)**, **Suspicious mshta process launched (Microsoft Defender for Endpoint)**, **Suspicious Process Discovery (Microsoft Defender for Endpoint)**, **Process execution from an alternate data stream (ADS) (Microsoft Defender for Endpoint)**, **Suspicious WMI process creation (Microsoft Defender for Endpoint)**, **Suspicious File and Directory Discovery (Microsoft Defender for Endpoint)**, **Suspicious Network Share Discovery (Microsoft Defender for Endpoint)**, **Suspicious remote PowerShell execution (Microsoft Defender for Endpoint)**, **A suspicious file was observed (Microsoft Defender for Endpoint)**, **Suspicious WMI activity initiated remotely (Microsoft Defender for Endpoint)**, **Suspicious file from a remote origin launched (Microsoft Defender for Endpoint)**, **Suspicious sequence of exploration activities (Microsoft Defender for Endpoint)**
- 2025-05-07T10:40:01.000Z: was communicated with by url hXXp://198[.]18[.]133[.]150:8000/attack[.]hta indicating **SID:1:29957:6 (TALOS)**, **Generic.Hacktool.BeEF.1.DE2EBF48 (null)**, **SID:1:15306:22 (TALOS)**, **SID:1:11192:20 (TALOS)**, **System file masquerade (Microsoft Defender for Endpoint)**, **SID:1:25276:10: Multiple products oversized Content-Length memory corruption attempt (TALOS)**, **SID:1:5708:13: web server file upload attempt (TALOS)**, **SID:1:23626:10 (TALOS)**, **SID:1:20619:6 (TALOS)**, **SID:1:38370:3 (TALOS)**, **SID:1:8068:17 (TALOS)**, **SID:1:42231:3: RTF url moniker COM file download attempt (TALOS)**, **SID:1:44416:3 (TALOS)**, **Suspicious PowerShell command line (Microsoft Defender for Endpoint)**, **SID:1:45745:3: CloudMe**

Sync Client stack buffer overflow attempt (TALOS), **Suspicious Endpoint Activity (XDR Endpoint)**, **Suspicious File Download Observed on Process Arguments - Suspicious Endpoint Activity (Cisco XDR)**, **Mshta Remote Payload Execution (Cisco Secure Endpoint)**, **Base64 Encoding Detected - Suspicious Endpoint Activity (Cisco XDR)**, **System Binary Executed from an Unusual Location - Suspicious Endpoint Activity (Cisco XDR)**, **Malicious Process Detected - Suspicious Endpoint Activity (Cisco XDR)**, **Suspicious mshta process launched (Microsoft Defender for Endpoint)**, **Suspicious Process Discovery (Microsoft Defender for Endpoint)**, **Process execution from an alternate data stream (ADS) (Microsoft Defender for Endpoint)**, **Suspicious WMI process creation (Microsoft Defender for Endpoint)**, **Suspicious File and Directory Discovery (Microsoft Defender for Endpoint)**, **Suspicious Network Share Discovery (Microsoft Defender for Endpoint)**, **Suspicious remote PowerShell execution (Microsoft Defender for Endpoint)**, **A suspicious file was observed (Microsoft Defender for Endpoint)**, **Suspicious WMI activity initiated remotely (Microsoft Defender for Endpoint)**, **Suspicious file from a remote origin launched (Microsoft Defender for Endpoint)**, **Suspicious sequence of exploration activities (Microsoft Defender for Endpoint)**

- 2025-05-07T10:40:01.000Z: was connected by process powershell[.]exe indicating **System file masquerade (Microsoft Defender for Endpoint)**, **Suspicious PowerShell command line (Microsoft Defender for Endpoint)**, **Suspicious Endpoint Activity (XDR Endpoint)**, **Base64 Encoding Detected - Suspicious Endpoint Activity (Cisco XDR)**, **System Binary Executed from an Unusual Location - Suspicious Endpoint Activity (Cisco XDR)**, **Malicious Process Detected - Suspicious Endpoint Activity (Cisco XDR)**, **Suspicious mshta process launched (Microsoft Defender for Endpoint)**, **Suspicious Process Discovery (Microsoft Defender for Endpoint)**, **Suspicious process executed PowerShell command (Microsoft Defender for Endpoint)**, **An active 'SandCat' malware process was detected while executing (Microsoft Defender for Endpoint)**, **Windows User Account Control Disabled In Registry (Cisco Secure Endpoint)**, **Mimikatz Dump Credentials Execution (Cisco Secure Endpoint)**, **PowerShell Exploitation Framework Commandlets (Cisco Secure Endpoint)**, **Mimikatz Dump Credentials (Cisco Secure Endpoint)**, **Command References Remote Red Team Tools (Cisco Secure Endpoint)**, **PowerShell Download String (Cisco Secure Endpoint)**, **Raw GitHub Argument (Cisco Secure Endpoint)**, **PowerShell Exploitation Framework Commandlets (IEX) (Cisco Secure Endpoint)**, **Read Process Memory of LSASS by PowerShell (Cisco Secure Endpoint)**, **Possible attempt to steal credentials (Microsoft Defender for Endpoint)**, **Suspicious System Hardware Discovery (Microsoft Defender for Endpoint)**, **Suspicious Network Share Discovery (Microsoft Defender for Endpoint)**, **Suspicious File and Directory Discovery (Microsoft Defender for Endpoint)**, **PowerView Module Loaded (Cisco Secure Endpoint)**, **Active Directory Enumeration of Unconstrained Delegation (Cisco Secure Endpoint)**, **Process execution from an alternate data stream (ADS) (Microsoft Defender for Endpoint)**, **Suspicious remote PowerShell execution (Microsoft Defender for Endpoint)**, **A suspicious file was observed (Microsoft Defender for Endpoint)**, **Suspicious WMI activity initiated remotely (Microsoft Defender for Endpoint)**, **Suspicious file from a remote origin launched (Microsoft Defender for Endpoint)**,

Suspicious sequence of exploration activities (Microsoft Defender for Endpoint), **Suspicious Use of Discovery Tools - Suspicious Endpoint Activity (Cisco XDR)** (3 times)

- 2025-05-07T10:40:01.000Z: was communicated with by url hXXps://download[.]sysinternals[.]com/files/PSTools[.]zip/ indicating **Suspicious PowerShell command line (Microsoft Defender for Endpoint)**, **A suspicious file was observed (Microsoft Defender for Endpoint)**, **Suspicious WMI activity initiated remotely (Microsoft Defender for Endpoint)**, **Suspicious file from a remote origin launched (Microsoft Defender for Endpoint)**, **Suspicious sequence of exploration activities (Microsoft Defender for Endpoint)**
- 2025-05-07T10:40:01.000Z: was observed on by process svchost[.]exe indicating **System file masquerade (Microsoft Defender for Endpoint)**, **Suspicious PowerShell command line (Microsoft Defender for Endpoint)**, **Suspicious Endpoint Activity (XDR Endpoint)**, **System Binary Executed from an Unusual Location - Suspicious Endpoint Activity (Cisco XDR)**, **Malicious Process Detected - Suspicious Endpoint Activity (Cisco XDR)**, **Suspicious Process Discovery (Microsoft Defender for Endpoint)**, **Suspicious process executed PowerShell command (Microsoft Defender for Endpoint)**, **An active 'SandCat' malware process was detected while executing (Microsoft Defender for Endpoint)**, **PowerShell Exploitation Framework Commandlets (Cisco Secure Endpoint)**, **Mimikatz Dump Credentials (Cisco Secure Endpoint)**, **Command References Remote Red Team Tools (Cisco Secure Endpoint)**, **PowerShell Download String (Cisco Secure Endpoint)**, **Raw GitHub Argument (Cisco Secure Endpoint)**, **Possible attempt to steal credentials (Microsoft Defender for Endpoint)**, **Suspicious System Hardware Discovery (Microsoft Defender for Endpoint)**, **Suspicious Network Share Discovery (Microsoft Defender for Endpoint)**, **Suspicious File and Directory Discovery (Microsoft Defender for Endpoint)**, **Process execution from an alternate data stream (ADS) (Microsoft Defender for Endpoint)**, **Suspicious WMI process creation (Microsoft Defender for Endpoint)**
- 2025-05-07T10:40:01.000Z: executed process svchost[.]exe indicating **System file masquerade (Microsoft Defender for Endpoint)**, **Suspicious PowerShell command line (Microsoft Defender for Endpoint)**, **Suspicious Endpoint Activity (XDR Endpoint)**, **System Binary Executed from an Unusual Location - Suspicious Endpoint Activity (Cisco XDR)**, **Malicious Process Detected - Suspicious Endpoint Activity (Cisco XDR)**, **Suspicious Process Discovery (Microsoft Defender for Endpoint)**, **Suspicious process executed PowerShell command (Microsoft Defender for Endpoint)**, **An active 'SandCat' malware process was detected while executing (Microsoft Defender for Endpoint)**, **PowerShell Exploitation Framework Commandlets (Cisco Secure Endpoint)**, **Mimikatz Dump Credentials (Cisco Secure Endpoint)**, **Command References Remote Red Team Tools (Cisco Secure Endpoint)**, **PowerShell Download String (Cisco Secure Endpoint)**, **Raw GitHub Argument (Cisco Secure Endpoint)**, **Possible attempt to steal credentials (Microsoft Defender for Endpoint)**, **Suspicious System Hardware Discovery (Microsoft Defender for Endpoint)**, **Suspicious Network Share Discovery (Microsoft Defender for Endpoint)**, **Suspicious File and Directory Discovery (Microsoft Defender for Endpoint)**, **Process execution from an alternate data stream (ADS) (Microsoft Defender for Endpoint)**,

Suspicious WMI process creation (Microsoft Defender for Endpoint) (2 times)

- 2025-05-07T10:40:01.000Z: communicated with process powershell[.]exe indicating **System file masquerade (Microsoft Defender for Endpoint)**, **Suspicious PowerShell command line (Microsoft Defender for Endpoint)**, **Suspicious Endpoint Activity (XDR Endpoint)**, **Base64 Encoding Detected - Suspicious Endpoint Activity (Cisco XDR)**, **System Binary Executed from an Unusual Location - Suspicious Endpoint Activity (Cisco XDR)**, **Malicious Process Detected - Suspicious Endpoint Activity (Cisco XDR)**, **Suspicious mshta process launched (Microsoft Defender for Endpoint)**, **Suspicious Process Discovery (Microsoft Defender for Endpoint)**, **Suspicious process executed PowerShell command (Microsoft Defender for Endpoint)**, **An active 'SandCat' malware process was detected while executing (Microsoft Defender for Endpoint)**, **Windows User Account Control Disabled In Registry (Cisco Secure Endpoint)**, **Mimikatz Dump Credentials Execution (Cisco Secure Endpoint)**, **PowerShell Exploitation Framework Commandlets (Cisco Secure Endpoint)**, **Mimikatz Dump Credentials (Cisco Secure Endpoint)**, **Command References Remote Red Team Tools (Cisco Secure Endpoint)**, **PowerShell Download String (Cisco Secure Endpoint)**, **Raw GitHub Argument (Cisco Secure Endpoint)**, **PowerShell Exploitation Framework Commandlets (IEX) (Cisco Secure Endpoint)**, **Read Process Memory of LSASS by PowerShell (Cisco Secure Endpoint)**, **Possible attempt to steal credentials (Microsoft Defender for Endpoint)**, **Suspicious System Hardware Discovery (Microsoft Defender for Endpoint)**, **Suspicious Network Share Discovery (Microsoft Defender for Endpoint)**, **Suspicious File and Directory Discovery (Microsoft Defender for Endpoint)**, **PowerView Module Loaded (Cisco Secure Endpoint)**, **Active Directory Enumeration of Unconstrained Delegation (Cisco Secure Endpoint)**, **Process execution from an alternate data stream (ADS) (Microsoft Defender for Endpoint)**, **Suspicious remote PowerShell execution (Microsoft Defender for Endpoint)**, **A suspicious file was observed (Microsoft Defender for Endpoint)**, **Suspicious WMI activity initiated remotely (Microsoft Defender for Endpoint)**, **Suspicious file from a remote origin launched (Microsoft Defender for Endpoint)**, **Suspicious sequence of exploration activities (Microsoft Defender for Endpoint)**, **Suspicious Use of Discovery Tools - Suspicious Endpoint Activity (Cisco XDR)** (2 times)
- 2025-05-07T10:40:01.000Z: executed process services[.]exe indicating **Suspicious Endpoint Activity (XDR Endpoint)**, **Mshta Remote Payload Execution (Cisco Secure Endpoint)**, **Windows User Account Control Disabled In Registry (Cisco Secure Endpoint)**, **Mimikatz Dump Credentials Execution (Cisco Secure Endpoint)**, **PowerShell Exploitation Framework Commandlets (Cisco Secure Endpoint)**, **Mimikatz Dump Credentials (Cisco Secure Endpoint)**, **Command References Remote Red Team Tools (Cisco Secure Endpoint)**, **PowerShell Download String (Cisco Secure Endpoint)**, **Raw GitHub Argument (Cisco Secure Endpoint)**, **PowerShell Exploitation Framework Commandlets (IEX) (Cisco Secure Endpoint)**, **Read Process Memory of LSASS by PowerShell (Cisco Secure Endpoint)**, **PowerView Module Loaded (Cisco Secure Endpoint)**, **Active Directory Enumeration of Unconstrained Delegation (Cisco Secure Endpoint)**, **Suspicious Process Discovery (Microsoft Defender for Endpoint)**, **Suspicious System Hardware Discovery (Microsoft Defender for Endpoint)**

- 2025-05-07T10:40:01.000Z: executed process powershell[.]exe indicating **System file masquerade (Microsoft Defender for Endpoint)**, **Suspicious PowerShell command line (Microsoft Defender for Endpoint)**, **Suspicious Endpoint Activity (XDR Endpoint)**, **Base64 Encoding Detected - Suspicious Endpoint Activity (Cisco XDR)**, **System Binary Executed from an Unusual Location - Suspicious Endpoint Activity (Cisco XDR)**, **Malicious Process Detected - Suspicious Endpoint Activity (Cisco XDR)**, **Suspicious mshta process launched (Microsoft Defender for Endpoint)**, **Suspicious Process Discovery (Microsoft Defender for Endpoint)**, **Suspicious process executed PowerShell command (Microsoft Defender for Endpoint)**, **An active 'SandCat' malware process was detected while executing (Microsoft Defender for Endpoint)**, **Windows User Account Control Disabled In Registry (Cisco Secure Endpoint)**, **Mimikatz Dump Credentials Execution (Cisco Secure Endpoint)**, **PowerShell Exploitation Framework Commandlets (Cisco Secure Endpoint)**, **Mimikatz Dump Credentials (Cisco Secure Endpoint)**, **Command References Remote Red Team Tools (Cisco Secure Endpoint)**, **PowerShell Download String (Cisco Secure Endpoint)**, **Raw GitHub Argument (Cisco Secure Endpoint)**, **PowerShell Exploitation Framework Commandlets (IEX) (Cisco Secure Endpoint)**, **Read Process Memory of LSASS by PowerShell (Cisco Secure Endpoint)**, **Possible attempt to steal credentials (Microsoft Defender for Endpoint)**, **Suspicious System Hardware Discovery (Microsoft Defender for Endpoint)**, **Suspicious Network Share Discovery (Microsoft Defender for Endpoint)**, **Suspicious File and Directory Discovery (Microsoft Defender for Endpoint)**, **PowerView Module Loaded (Cisco Secure Endpoint)**, **Active Directory Enumeration of Unconstrained Delegation (Cisco Secure Endpoint)**, **Process execution from an alternate data stream (ADS) (Microsoft Defender for Endpoint)**, **Suspicious remote PowerShell execution (Microsoft Defender for Endpoint)**, **A suspicious file was observed (Microsoft Defender for Endpoint)**, **Suspicious WMI activity initiated remotely (Microsoft Defender for Endpoint)**, **Suspicious file from a remote origin launched (Microsoft Defender for Endpoint)**, **Suspicious sequence of exploration activities (Microsoft Defender for Endpoint)**, **Suspicious Use of Discovery Tools - Suspicious Endpoint Activity (Cisco XDR)** (3 times)
- 2025-05-07T10:40:01.000Z: used by user vic indicating **Suspicious Endpoint Activity (XDR Endpoint)**, **Mshta Remote Payload Execution (Cisco Secure Endpoint)**, **Windows User Account Control Disabled In Registry (Cisco Secure Endpoint)**, **Mimikatz Dump Credentials Execution (Cisco Secure Endpoint)**, **PowerShell Exploitation Framework Commandlets (Cisco Secure Endpoint)**, **Mimikatz Dump Credentials (Cisco Secure Endpoint)**, **Command References Remote Red Team Tools (Cisco Secure Endpoint)**, **PowerShell Download String (Cisco Secure Endpoint)**, **Raw GitHub Argument (Cisco Secure Endpoint)**, **PowerShell Exploitation Framework Commandlets (IEX) (Cisco Secure Endpoint)**, **Read Process Memory of LSASS by PowerShell (Cisco Secure Endpoint)**, **PowerView Module Loaded (Cisco Secure Endpoint)**, **Active Directory Enumeration of Unconstrained Delegation (Cisco Secure Endpoint)**
- 2025-05-07T10:40:01.000Z: accessed process svchost[.]exe indicating **System file masquerade (Microsoft Defender for Endpoint)**, **Suspicious PowerShell command line (Microsoft Defender for Endpoint)**, **Suspicious Endpoint Activity (XDR Endpoint)**, **System**

Binary Executed from an Unusual Location - Suspicious Endpoint Activity (Cisco XDR), **Malicious Process Detected - Suspicious Endpoint Activity (Cisco XDR)**, **Suspicious Process Discovery (Microsoft Defender for Endpoint)**, **Suspicious process executed PowerShell command (Microsoft Defender for Endpoint)**, **An active 'SandCat' malware process was detected while executing (Microsoft Defender for Endpoint)**, **PowerShell Exploitation Framework Commandlets (Cisco Secure Endpoint)**, **Mimikatz Dump Credentials (Cisco Secure Endpoint)**, **Command References Remote Red Team Tools (Cisco Secure Endpoint)**, **PowerShell Download String (Cisco Secure Endpoint)**, **Raw GitHub Argument (Cisco Secure Endpoint)**, **Possible attempt to steal credentials (Microsoft Defender for Endpoint)**, **Suspicious System Hardware Discovery (Microsoft Defender for Endpoint)**, **Suspicious Network Share Discovery (Microsoft Defender for Endpoint)**, **Suspicious File and Directory Discovery (Microsoft Defender for Endpoint)**, **Process execution from an alternate data stream (ADS) (Microsoft Defender for Endpoint)**, **Suspicious WMI process creation (Microsoft Defender for Endpoint)**

- 2025-05-07T10:40:01.000Z: communicated with process nslookup[.]exe indicating **Suspicious Use of Discovery Tools - Suspicious Endpoint Activity (Cisco XDR)** (6 times)
- 2025-05-07T10:40:01.000Z: communicated with process svchost[.]exe indicating **System file masquerade (Microsoft Defender for Endpoint)**, **Suspicious PowerShell command line (Microsoft Defender for Endpoint)**, **Suspicious Endpoint Activity (XDR Endpoint)**, **System Binary Executed from an Unusual Location - Suspicious Endpoint Activity (Cisco XDR)**, **Malicious Process Detected - Suspicious Endpoint Activity (Cisco XDR)**, **Suspicious Process Discovery (Microsoft Defender for Endpoint)**, **Suspicious process executed PowerShell command (Microsoft Defender for Endpoint)**, **An active 'SandCat' malware process was detected while executing (Microsoft Defender for Endpoint)**, **PowerShell Exploitation Framework Commandlets (Cisco Secure Endpoint)**, **Mimikatz Dump Credentials (Cisco Secure Endpoint)**, **Command References Remote Red Team Tools (Cisco Secure Endpoint)**, **PowerShell Download String (Cisco Secure Endpoint)**, **Raw GitHub Argument (Cisco Secure Endpoint)**, **Possible attempt to steal credentials (Microsoft Defender for Endpoint)**, **Suspicious System Hardware Discovery (Microsoft Defender for Endpoint)**, **Suspicious Network Share Discovery (Microsoft Defender for Endpoint)**, **Suspicious File and Directory Discovery (Microsoft Defender for Endpoint)**, **Process execution from an alternate data stream (ADS) (Microsoft Defender for Endpoint)**, **Suspicious WMI process creation (Microsoft Defender for Endpoint)**
- 2025-05-07T10:40:01.000Z: communicated with process mshta[.]exe indicating **System file masquerade (Microsoft Defender for Endpoint)**, **Suspicious PowerShell command line (Microsoft Defender for Endpoint)**, **Suspicious Endpoint Activity (XDR Endpoint)**, **Suspicious File Download Observed on Process Arguments - Suspicious Endpoint Activity (Cisco XDR)**, **Mshta Remote Payload Execution (Cisco Secure Endpoint)**, **Base64 Encoding Detected - Suspicious Endpoint Activity (Cisco XDR)**, **Suspicious mshta process launched (Microsoft Defender for Endpoint)**, **Suspicious Process Discovery (Microsoft Defender for Endpoint)**, **Suspicious process executed PowerShell command (Microsoft Defender for Endpoint)**

- 2025-05-07T10:40:01.000Z: connected to ip 198[.]18[.]133[.]150 indicating **SID:1:29957:6 (TALOS)**, **Generic.Hacktool.BeEF.1.DE2EBF48 (null)**, **SID:1:15306:22 (TALOS)**, **SID:1:11192:20 (TALOS)**, **System file masquerade (Microsoft Defender for Endpoint)**, **SID:1:25276:10: Multiple products oversized Content-Length memory corruption attempt (TALOS)**, **SID:1:5708:13: web server file upload attempt (TALOS)**, **SID:1:23626:10 (TALOS)**, **SID:1:20619:6 (TALOS)**, **SID:1:38370:3 (TALOS)**, **SID:1:8068:17 (TALOS)**, **SID:1:42231:3: RTF url moniker COM file download attempt (TALOS)**, **SID:1:44416:3 (TALOS)**, **Suspicious PowerShell command line (Microsoft Defender for Endpoint)**, **SID:1:45745:3: CloudMe Sync Client stack buffer overflow attempt (TALOS)**, **Suspicious Endpoint Activity (XDR Endpoint)**, **Suspicious File Download Observed on Process Arguments - Suspicious Endpoint Activity (Cisco XDR)**, **Mshta Remote Payload Execution (Cisco Secure Endpoint)**, **Base64 Encoding Detected - Suspicious Endpoint Activity (Cisco XDR)**, **System Binary Executed from an Unusual Location - Suspicious Endpoint Activity (Cisco XDR)**, **Malicious Process Detected - Suspicious Endpoint Activity (Cisco XDR)**, **Suspicious mshta process launched (Microsoft Defender for Endpoint)**, **Suspicious Process Discovery (Microsoft Defender for Endpoint)**, **Process execution from an alternate data stream (ADS) (Microsoft Defender for Endpoint)**, **Suspicious WMI process creation (Microsoft Defender for Endpoint)**, **Suspicious File and Directory Discovery (Microsoft Defender for Endpoint)**, **Suspicious Network Share Discovery (Microsoft Defender for Endpoint)**, **Suspicious remote PowerShell execution (Microsoft Defender for Endpoint)**, **A suspicious file was observed (Microsoft Defender for Endpoint)**, **Suspicious WMI activity initiated remotely (Microsoft Defender for Endpoint)**, **Suspicious file from a remote origin launched (Microsoft Defender for Endpoint)**, **Suspicious sequence of exploration activities (Microsoft Defender for Endpoint)**
- 2025-05-07T10:40:01.000Z: executed process powershell[.]exe indicating **System file masquerade (Microsoft Defender for Endpoint)**, **Suspicious PowerShell command line (Microsoft Defender for Endpoint)**, **Suspicious Endpoint Activity (XDR Endpoint)**, **Base64 Encoding Detected - Suspicious Endpoint Activity (Cisco XDR)**, **System Binary Executed from an Unusual Location - Suspicious Endpoint Activity (Cisco XDR)**, **Malicious Process Detected - Suspicious Endpoint Activity (Cisco XDR)**, **Suspicious mshta process launched (Microsoft Defender for Endpoint)**, **Suspicious Process Discovery (Microsoft Defender for Endpoint)**, **Suspicious process executed PowerShell command (Microsoft Defender for Endpoint)**, **An active 'SandCat' malware process was detected while executing (Microsoft Defender for Endpoint)**, **Windows User Account Control Disabled In Registry (Cisco Secure Endpoint)**, **Mimikatz Dump Credentials Execution (Cisco Secure Endpoint)**, **PowerShell Exploitation Framework Commandlets (Cisco Secure Endpoint)**, **Mimikatz Dump Credentials (Cisco Secure Endpoint)**, **Command References Remote Red Team Tools (Cisco Secure Endpoint)**, **PowerShell Download String (Cisco Secure Endpoint)**, **Raw GitHub Argument (Cisco Secure Endpoint)**, **PowerShell Exploitation Framework Commandlets (IEX) (Cisco Secure Endpoint)**, **Read Process Memory of LSASS by PowerShell (Cisco Secure Endpoint)**, **Possible attempt to steal credentials (Microsoft Defender for Endpoint)**, **Suspicious System Hardware Discovery (Microsoft Defender for**

Endpoint), **Suspicious Network Share Discovery (Microsoft Defender for Endpoint)**, **Suspicious File and Directory Discovery (Microsoft Defender for Endpoint)**, **PowerView Module Loaded (Cisco Secure Endpoint)**, **Active Directory Enumeration of Unconstrained Delegation (Cisco Secure Endpoint)**, **Process execution from an alternate data stream (ADS) (Microsoft Defender for Endpoint)**, **Suspicious remote PowerShell execution (Microsoft Defender for Endpoint)**, **A suspicious file was observed (Microsoft Defender for Endpoint)**, **Suspicious WMI activity initiated remotely (Microsoft Defender for Endpoint)**, **Suspicious file from a remote origin launched (Microsoft Defender for Endpoint)**, **Suspicious sequence of exploration activities (Microsoft Defender for Endpoint)**, **Suspicious Use of Discovery Tools - Suspicious Endpoint Activity (Cisco XDR)**

- 2025-05-07T10:40:01.000Z: executed process svchost[.]exe indicating **System file masquerade (Microsoft Defender for Endpoint)**, **Suspicious PowerShell command line (Microsoft Defender for Endpoint)**, **Suspicious Endpoint Activity (XDR Endpoint)**, **System Binary Executed from an Unusual Location - Suspicious Endpoint Activity (Cisco XDR)**, **Malicious Process Detected - Suspicious Endpoint Activity (Cisco XDR)**, **Suspicious Process Discovery (Microsoft Defender for Endpoint)**, **Suspicious process executed PowerShell command (Microsoft Defender for Endpoint)**, **An active 'SandCat' malware process was detected while executing (Microsoft Defender for Endpoint)**, **PowerShell Exploitation Framework Commandlets (Cisco Secure Endpoint)**, **Mimikatz Dump Credentials (Cisco Secure Endpoint)**, **Command References Remote Red Team Tools (Cisco Secure Endpoint)**, **PowerShell Download String (Cisco Secure Endpoint)**, **Raw GitHub Argument (Cisco Secure Endpoint)**, **Possible attempt to steal credentials (Microsoft Defender for Endpoint)**, **Suspicious System Hardware Discovery (Microsoft Defender for Endpoint)**, **Suspicious Network Share Discovery (Microsoft Defender for Endpoint)**, **Suspicious File and Directory Discovery (Microsoft Defender for Endpoint)**, **Process execution from an alternate data stream (ADS) (Microsoft Defender for Endpoint)**, **Suspicious WMI process creation (Microsoft Defender for Endpoint)**
- 2025-05-07T10:40:01.000Z: connected to url hXXp://attacker[.]ihatemikesimone[.]com:8888/ indicating **Suspicious Endpoint Activity (XDR Endpoint)**, **Suspicious File Download Observed on Process Arguments - Suspicious Endpoint Activity (Cisco XDR)**, **Base64 Encoding Detected - Suspicious Endpoint Activity (Cisco XDR)**, **System Binary Executed from an Unusual Location - Suspicious Endpoint Activity (Cisco XDR)**, **Malicious Process Detected - Suspicious Endpoint Activity (Cisco XDR)**, **System file masquerade (Microsoft Defender for Endpoint)**, **Suspicious Process Discovery (Microsoft Defender for Endpoint)**, **An active 'SandCat' malware process was detected while executing (Microsoft Defender for Endpoint)**, **PowerShell Exploitation Framework Commandlets (Cisco Secure Endpoint)**, **Mimikatz Dump Credentials (Cisco Secure Endpoint)**, **Command References Remote Red Team Tools (Cisco Secure Endpoint)**, **PowerShell Download String (Cisco Secure Endpoint)**, **Raw GitHub Argument (Cisco Secure Endpoint)**, **Suspicious PowerShell command line (Microsoft Defender for Endpoint)**, **Suspicious Network Share Discovery (Microsoft Defender for Endpoint)**, **Suspicious File and Directory Discovery (Microsoft Defender for Endpoint)**, **Suspicious**

remote PowerShell execution (Microsoft Defender for Endpoint), **A suspicious file was observed (Microsoft Defender for Endpoint)**, **Suspicious WMI activity initiated remotely (Microsoft Defender for Endpoint)**, **Suspicious file from a remote origin launched (Microsoft Defender for Endpoint)**, **Suspicious sequence of exploration activities (Microsoft Defender for Endpoint)**

- 2025-05-07T10:40:01.000Z: connected to ip 198[.]19[.]255[.]146 indicating **System file masquerade (Microsoft Defender for Endpoint)**, **Suspicious PowerShell command line (Microsoft Defender for Endpoint)**, **Suspicious mshta process launched (Microsoft Defender for Endpoint)**, **Suspicious Process Discovery (Microsoft Defender for Endpoint)**, **Suspicious process executed PowerShell command (Microsoft Defender for Endpoint)**, **An active 'SandCat' malware process was detected while executing (Microsoft Defender for Endpoint)**, **Suspicious Network Share Discovery (Microsoft Defender for Endpoint)**, **Suspicious File and Directory Discovery (Microsoft Defender for Endpoint)**
- 2025-05-07T10:40:01.000Z: connected to url hXXp://198[.]18[.]133[.]150:8000/attack[.]hta indicating **SID:1:29957:6 (TALOS)**, **Generic.Hacktool.BeEF.1.DE2EBF48 (null)**, **SID:1:15306:22 (TALOS)**, **SID:1:11192:20 (TALOS)**, **System file masquerade (Microsoft Defender for Endpoint)**, **SID:1:25276:10: Multiple products oversized Content-Length memory corruption attempt (TALOS)**, **SID:1:5708:13: web server file upload attempt (TALOS)**, **SID:1:23626:10 (TALOS)**, **SID:1:20619:6 (TALOS)**, **SID:1:38370:3 (TALOS)**, **SID:1:8068:17 (TALOS)**, **SID:1:42231:3: RTF url moniker COM file download attempt (TALOS)**, **SID:1:44416:3 (TALOS)**, **Suspicious PowerShell command line (Microsoft Defender for Endpoint)**, **SID:1:45745:3: CloudMe Sync Client stack buffer overflow attempt (TALOS)**, **Suspicious Endpoint Activity (XDR Endpoint)**, **Suspicious File Download Observed on Process Arguments - Suspicious Endpoint Activity (Cisco XDR)**, **Mshta Remote Payload Execution (Cisco Secure Endpoint)**, **Base64 Encoding Detected - Suspicious Endpoint Activity (Cisco XDR)**, **System Binary Executed from an Unusual Location - Suspicious Endpoint Activity (Cisco XDR)**, **Malicious Process Detected - Suspicious Endpoint Activity (Cisco XDR)**, **Suspicious mshta process launched (Microsoft Defender for Endpoint)**, **Suspicious Process Discovery (Microsoft Defender for Endpoint)**, **Process execution from an alternate data stream (ADS) (Microsoft Defender for Endpoint)**, **Suspicious WMI process creation (Microsoft Defender for Endpoint)**, **Suspicious File and Directory Discovery (Microsoft Defender for Endpoint)**, **Suspicious Network Share Discovery (Microsoft Defender for Endpoint)**, **Suspicious remote PowerShell execution (Microsoft Defender for Endpoint)**, **A suspicious file was observed (Microsoft Defender for Endpoint)**, **Suspicious WMI activity initiated remotely (Microsoft Defender for Endpoint)**, **Suspicious file from a remote origin launched (Microsoft Defender for Endpoint)**, **Suspicious sequence of exploration activities (Microsoft Defender for Endpoint)**
- 2025-05-07T10:40:01.000Z: connected to url hXXps://download[.]sysinternals[.]com/files/PSTools[.]zip/ indicating **Suspicious PowerShell command line (Microsoft Defender for Endpoint)**, **A suspicious file was observed (Microsoft Defender for Endpoint)**, **Suspicious WMI activity initiated remotely (Microsoft Defender for Endpoint)**, **Suspicious file from a remote origin launched (Microsoft Defender for Endpoint)**, **Suspicious sequence of**

exploration activities (Microsoft Defender for Endpoint)

- 2025-05-07T10:40:01.000Z: executed process nslookup[.]exe indicating **Suspicious Use of Discovery Tools - Suspicious Endpoint Activity (Cisco XDR)** (6 times)
- 2025-05-07T10:40:01.000Z: communicated with device Vic indicating **Suspicious Endpoint Activity (XDR Endpoint)**, **Mshta Remote Payload Execution (Cisco Secure Endpoint)**, **Windows User Account Control Disabled In Registry (Cisco Secure Endpoint)**, **Mimikatz Dump Credentials Execution (Cisco Secure Endpoint)**, **PowerShell Exploitation Framework Commandlets (Cisco Secure Endpoint)**, **Mimikatz Dump Credentials (Cisco Secure Endpoint)**, **Command References Remote Red Team Tools (Cisco Secure Endpoint)**, **PowerShell Download String (Cisco Secure Endpoint)**, **Raw GitHub Argument (Cisco Secure Endpoint)**, **PowerShell Exploitation Framework Commandlets (IEX) (Cisco Secure Endpoint)**, **Read Process Memory of LSASS by PowerShell (Cisco Secure Endpoint)**, **PowerView Module Loaded (Cisco Secure Endpoint)**, **Active Directory Enumeration of Unconstrained Delegation (Cisco Secure Endpoint)**
- 2025-05-07T10:40:01.000Z: connected to url hXXp://198[.]18[.]133[.]150:8888/ indicating **SID:1:29957:6 (TALOS)**, **Generic.Hacktool.BeEF.1.DE2EBF48 (null)**, **SID:1:15306:22 (TALOS)**, **SID:1:11192:20 (TALOS)**, **System file masquerade (Microsoft Defender for Endpoint)**, **SID:1:25276:10: Multiple products oversized Content-Length memory corruption attempt (TALOS)**, **SID:1:5708:13: web server file upload attempt (TALOS)**, **SID:1:23626:10 (TALOS)**, **SID:1:20619:6 (TALOS)**, **SID:1:38370:3 (TALOS)**, **SID:1:8068:17 (TALOS)**, **SID:1:42231:3: RTF url moniker COM file download attempt (TALOS)**, **SID:1:44416:3 (TALOS)**, **Suspicious PowerShell command line (Microsoft Defender for Endpoint)**, **SID:1:45745:3: CloudMe Sync Client stack buffer overflow attempt (TALOS)**, **Suspicious Endpoint Activity (XDR Endpoint)**, **Suspicious File Download Observed on Process Arguments - Suspicious Endpoint Activity (Cisco XDR)**, **Mshta Remote Payload Execution (Cisco Secure Endpoint)**, **Base64 Encoding Detected - Suspicious Endpoint Activity (Cisco XDR)**, **System Binary Executed from an Unusual Location - Suspicious Endpoint Activity (Cisco XDR)**, **Malicious Process Detected - Suspicious Endpoint Activity (Cisco XDR)**, **Suspicious mshta process launched (Microsoft Defender for Endpoint)**, **Suspicious Process Discovery (Microsoft Defender for Endpoint)**, **Process execution from an alternate data stream (ADS) (Microsoft Defender for Endpoint)**, **Suspicious WMI process creation (Microsoft Defender for Endpoint)**, **Suspicious File and Directory Discovery (Microsoft Defender for Endpoint)**, **Suspicious Network Share Discovery (Microsoft Defender for Endpoint)**, **Suspicious remote PowerShell execution (Microsoft Defender for Endpoint)**, **A suspicious file was observed (Microsoft Defender for Endpoint)**, **Suspicious WMI activity initiated remotely (Microsoft Defender for Endpoint)**, **Suspicious file from a remote origin launched (Microsoft Defender for Endpoint)**, **Suspicious sequence of exploration activities (Microsoft Defender for Endpoint)**
- 2025-05-07T10:40:01.000Z: communicated with process powershell[.]exe indicating **System file masquerade (Microsoft Defender for Endpoint)**, **Suspicious PowerShell command line (Microsoft Defender for Endpoint)**, **Suspicious Endpoint Activity (XDR Endpoint)**, **Base64 Encoding Detected - Suspicious Endpoint Activity (Cisco XDR)**, **System Binary Executed**

from an Unusual Location - Suspicious Endpoint Activity (Cisco XDR), **Malicious Process Detected - Suspicious Endpoint Activity (Cisco XDR)**, **Suspicious mshta process launched (Microsoft Defender for Endpoint)**, **Suspicious Process Discovery (Microsoft Defender for Endpoint)**, **Suspicious process executed PowerShell command (Microsoft Defender for Endpoint)**, **An active 'SandCat' malware process was detected while executing (Microsoft Defender for Endpoint)**, **Windows User Account Control Disabled In Registry (Cisco Secure Endpoint)**, **Mimikatz Dump Credentials Execution (Cisco Secure Endpoint)**, **PowerShell Exploitation Framework Commandlets (Cisco Secure Endpoint)**, **Mimikatz Dump Credentials (Cisco Secure Endpoint)**, **Command References Remote Red Team Tools (Cisco Secure Endpoint)**, **PowerShell Download String (Cisco Secure Endpoint)**, **Raw GitHub Argument (Cisco Secure Endpoint)**, **PowerShell Exploitation Framework Commandlets (IEX) (Cisco Secure Endpoint)**, **Read Process Memory of LSASS by PowerShell (Cisco Secure Endpoint)**, **Possible attempt to steal credentials (Microsoft Defender for Endpoint)**, **Suspicious System Hardware Discovery (Microsoft Defender for Endpoint)**, **Suspicious Network Share Discovery (Microsoft Defender for Endpoint)**, **Suspicious File and Directory Discovery (Microsoft Defender for Endpoint)**, **PowerView Module Loaded (Cisco Secure Endpoint)**, **Active Directory Enumeration of Unconstrained Delegation (Cisco Secure Endpoint)**, **Process execution from an alternate data stream (ADS) (Microsoft Defender for Endpoint)**, **Suspicious remote PowerShell execution (Microsoft Defender for Endpoint)**, **A suspicious file was observed (Microsoft Defender for Endpoint)**, **Suspicious WMI activity initiated remotely (Microsoft Defender for Endpoint)**, **Suspicious file from a remote origin launched (Microsoft Defender for Endpoint)**, **Suspicious sequence of exploration activities (Microsoft Defender for Endpoint)**, **Suspicious Use of Discovery Tools - Suspicious Endpoint Activity (Cisco XDR)** (2 times)

- 2025-05-07T10:40:01.000Z: executed process powershell[.]exe indicating **System file masquerade (Microsoft Defender for Endpoint)**, **Suspicious PowerShell command line (Microsoft Defender for Endpoint)**, **Suspicious Endpoint Activity (XDR Endpoint)**, **Base64 Encoding Detected - Suspicious Endpoint Activity (Cisco XDR)**, **System Binary Executed from an Unusual Location - Suspicious Endpoint Activity (Cisco XDR)**, **Malicious Process Detected - Suspicious Endpoint Activity (Cisco XDR)**, **Suspicious mshta process launched (Microsoft Defender for Endpoint)**, **Suspicious Process Discovery (Microsoft Defender for Endpoint)**, **Suspicious process executed PowerShell command (Microsoft Defender for Endpoint)**, **An active 'SandCat' malware process was detected while executing (Microsoft Defender for Endpoint)**, **Windows User Account Control Disabled In Registry (Cisco Secure Endpoint)**, **Mimikatz Dump Credentials Execution (Cisco Secure Endpoint)**, **PowerShell Exploitation Framework Commandlets (Cisco Secure Endpoint)**, **Mimikatz Dump Credentials (Cisco Secure Endpoint)**, **Command References Remote Red Team Tools (Cisco Secure Endpoint)**, **PowerShell Download String (Cisco Secure Endpoint)**, **Raw GitHub Argument (Cisco Secure Endpoint)**, **PowerShell Exploitation Framework Commandlets (IEX) (Cisco Secure Endpoint)**, **Read Process Memory of LSASS by PowerShell (Cisco Secure Endpoint)**, **Possible attempt to steal credentials (Microsoft Defender for Endpoint)**, **Suspicious System Hardware Discovery (Microsoft Defender for**

Endpoint), **Suspicious Network Share Discovery (Microsoft Defender for Endpoint)**, **Suspicious File and Directory Discovery (Microsoft Defender for Endpoint)**, **PowerView Module Loaded (Cisco Secure Endpoint)**, **Active Directory Enumeration of Unconstrained Delegation (Cisco Secure Endpoint)**, **Process execution from an alternate data stream (ADS) (Microsoft Defender for Endpoint)**, **Suspicious remote PowerShell execution (Microsoft Defender for Endpoint)**, **A suspicious file was observed (Microsoft Defender for Endpoint)**, **Suspicious WMI activity initiated remotely (Microsoft Defender for Endpoint)**, **Suspicious file from a remote origin launched (Microsoft Defender for Endpoint)**, **Suspicious sequence of exploration activities (Microsoft Defender for Endpoint)**, **Suspicious Use of Discovery Tools - Suspicious Endpoint Activity (Cisco XDR)**

- 2025-05-07T10:40:01.000Z: executed process svchost[.]exe indicating **System file masquerade (Microsoft Defender for Endpoint)**, **Suspicious PowerShell command line (Microsoft Defender for Endpoint)**, **Suspicious Endpoint Activity (XDR Endpoint)**, **System Binary Executed from an Unusual Location - Suspicious Endpoint Activity (Cisco XDR)**, **Malicious Process Detected - Suspicious Endpoint Activity (Cisco XDR)**, **Suspicious Process Discovery (Microsoft Defender for Endpoint)**, **Suspicious process executed PowerShell command (Microsoft Defender for Endpoint)**, **An active 'SandCat' malware process was detected while executing (Microsoft Defender for Endpoint)**, **PowerShell Exploitation Framework Commandlets (Cisco Secure Endpoint)**, **Mimikatz Dump Credentials (Cisco Secure Endpoint)**, **Command References Remote Red Team Tools (Cisco Secure Endpoint)**, **PowerShell Download String (Cisco Secure Endpoint)**, **Raw GitHub Argument (Cisco Secure Endpoint)**, **Possible attempt to steal credentials (Microsoft Defender for Endpoint)**, **Suspicious System Hardware Discovery (Microsoft Defender for Endpoint)**, **Suspicious Network Share Discovery (Microsoft Defender for Endpoint)**, **Suspicious File and Directory Discovery (Microsoft Defender for Endpoint)**, **Process execution from an alternate data stream (ADS) (Microsoft Defender for Endpoint)**, **Suspicious WMI process creation (Microsoft Defender for Endpoint)**
- 2025-05-07T10:40:01.000Z: executed process mshta[.]exe indicating **System file masquerade (Microsoft Defender for Endpoint)**, **Suspicious PowerShell command line (Microsoft Defender for Endpoint)**, **Suspicious Endpoint Activity (XDR Endpoint)**, **Suspicious File Download Observed on Process Arguments - Suspicious Endpoint Activity (Cisco XDR)**, **Mshta Remote Payload Execution (Cisco Secure Endpoint)**, **Base64 Encoding Detected - Suspicious Endpoint Activity (Cisco XDR)**, **Suspicious mshta process launched (Microsoft Defender for Endpoint)**, **Suspicious Process Discovery (Microsoft Defender for Endpoint)**, **Suspicious process executed PowerShell command (Microsoft Defender for Endpoint)** (4 times)
- 2025-05-07T10:40:01.000Z: executed process iexplore[.]exe indicating **Generic.Hacktool.BeEF.1.DE2EBF48 (null)**, **Suspicious PowerShell command line (Microsoft Defender for Endpoint)**, **Mshta Remote Payload Execution (Cisco Secure Endpoint)**, **Suspicious mshta process launched (Microsoft Defender for Endpoint)**, **Suspicious Process Discovery (Microsoft Defender for Endpoint)**
- 2025-05-07T10:40:01.000Z: accessed files cryptdll[.]dll, samlib[.]dll, WinSCard.dll and 2

more indicating **Possible attempt to steal credentials (Microsoft Defender for Endpoint)**
- 2025-05-07T10:40:01.000Z: executed process powershell[.]exe indicating **System file masquerade (Microsoft Defender for Endpoint)**, **Suspicious PowerShell command line (Microsoft Defender for Endpoint)**, **Suspicious Endpoint Activity (XDR Endpoint)**, **Base64 Encoding Detected - Suspicious Endpoint Activity (Cisco XDR)**, **System Binary Executed from an Unusual Location - Suspicious Endpoint Activity (Cisco XDR)**, **Malicious Process Detected - Suspicious Endpoint Activity (Cisco XDR)**, **Suspicious mshta process launched (Microsoft Defender for Endpoint)**, **Suspicious Process Discovery (Microsoft Defender for Endpoint)**, **Suspicious process executed PowerShell command (Microsoft Defender for Endpoint)**, **An active 'SandCat' malware process was detected while executing (Microsoft Defender for Endpoint)**, **Windows User Account Control Disabled In Registry (Cisco Secure Endpoint)**, **Mimikatz Dump Credentials Execution (Cisco Secure Endpoint)**, **PowerShell Exploitation Framework Commandlets (Cisco Secure Endpoint)**, **Mimikatz Dump Credentials (Cisco Secure Endpoint)**, **Command References Remote Red Team Tools (Cisco Secure Endpoint)**, **PowerShell Download String (Cisco Secure Endpoint)**, **Raw GitHub Argument (Cisco Secure Endpoint)**, **PowerShell Exploitation Framework Commandlets (IEX) (Cisco Secure Endpoint)**, **Read Process Memory of LSASS by PowerShell (Cisco Secure Endpoint)**, **Possible attempt to steal credentials (Microsoft Defender for Endpoint)**, **Suspicious System Hardware Discovery (Microsoft Defender for Endpoint)**, **Suspicious Network Share Discovery (Microsoft Defender for Endpoint)**, **Suspicious File and Directory Discovery (Microsoft Defender for Endpoint)**, **PowerView Module Loaded (Cisco Secure Endpoint)**, **Active Directory Enumeration of Unconstrained Delegation (Cisco Secure Endpoint)**, **Process execution from an alternate data stream (ADS) (Microsoft Defender for Endpoint)**, **Suspicious remote PowerShell execution (Microsoft Defender for Endpoint)**, **A suspicious file was observed (Microsoft Defender for Endpoint)**, **Suspicious WMI activity initiated remotely (Microsoft Defender for Endpoint)**, **Suspicious file from a remote origin launched (Microsoft Defender for Endpoint)**, **Suspicious sequence of exploration activities (Microsoft Defender for Endpoint)**, **Suspicious Use of Discovery Tools - Suspicious Endpoint Activity (Cisco XDR)** (12 times)

7. user NT AUTHORITY/SYSTEM
    - 2025-09-22T04:02:15.000Z: executed process svchost[.]exe indicating **Suspicious Process Discovery (Microsoft Defender for Endpoint)**, **Suspicious System Hardware Discovery (Microsoft Defender for Endpoint)**
    - 2025-09-24T09:39:12.492Z: assigned to device dc01[.]xdri[.]local
    - 2025-09-24T09:39:12.492Z: executed process lsass[.]exe indicating **Suspicious remote PowerShell execution (Microsoft Defender for Endpoint)**, **A suspicious file was observed (Microsoft Defender for Endpoint)**, **Suspicious WMI activity initiated remotely (Microsoft Defender for Endpoint)**, **Suspicious file from a remote origin launched (Microsoft Defender for Endpoint)**, **Suspicious sequence of exploration activities (Microsoft Defender for Endpoint)**, **Suspicious PowerShell command line (Microsoft Defender for Endpoint)**
8. user NETWORK SERVICE
    - 2025-09-24T09:39:12.492Z: accessed device dc01[.]xdri[.]local

- 2025-09-24T09:39:12.492Z: executed process WmiPrvSE.exe
- 2025-09-27T10:49:04.000Z: was used by process WmiPrvSE.exe
- 2025-09-27T10:49:04.000Z: executed process WmiPrvSE.exe (2 times)

9. user SYSTEM
   - 2025-09-22T04:02:19.588Z: was used by process svchost[.]exe indicating **Suspicious Process Discovery (Microsoft Defender for Endpoint)**, **Suspicious System Hardware Discovery (Microsoft Defender for Endpoint)**
   - 2025-09-22T04:02:19.588Z: executed process svchost[.]exe indicating **Suspicious Process Discovery (Microsoft Defender for Endpoint)**, **Suspicious System Hardware Discovery (Microsoft Defender for Endpoint)**
   - 2025-09-28T04:20:55.746Z: was used by process lsass[.]exe indicating **Suspicious remote PowerShell execution (Microsoft Defender for Endpoint)**, **A suspicious file was observed (Microsoft Defender for Endpoint)**, **Suspicious WMI activity initiated remotely (Microsoft Defender for Endpoint)**, **Suspicious file from a remote origin launched (Microsoft Defender for Endpoint)**, **Suspicious sequence of exploration activities (Microsoft Defender for Endpoint)**, **Suspicious PowerShell command line (Microsoft Defender for Endpoint)**
   - 2025-09-28T04:20:55.746Z: executed process lsass[.]exe indicating **Suspicious remote PowerShell execution (Microsoft Defender for Endpoint)**, **A suspicious file was observed (Microsoft Defender for Endpoint)**, **Suspicious WMI activity initiated remotely (Microsoft Defender for Endpoint)**, **Suspicious file from a remote origin launched (Microsoft Defender for Endpoint)**, **Suspicious sequence of exploration activities (Microsoft Defender for Endpoint)**, **Suspicious PowerShell command line (Microsoft Defender for Endpoint)**

Incident Timeline

May 07, 2025

- **10:40:01 -** Asset/Incident Responder: device Vic **-** Actions: was observed on by process svchost[.]exe
- **10:40:01 -** Asset/Incident Responder: device Vic **-** Actions: was communicated with by ip 198[.]18[.]133[.]150
- **10:40:01 -** Asset/Incident Responder: device Vic **-** Actions: was observed on by process svchost[.]exe (3 times)
- **10:40:01 -** Asset/Incident Responder: device Vic **-** Actions: was communicated with by hostname attacker[.]ihatemikesimone[.]com
- **10:40:01 -** Asset/Incident Responder: device Vic **-** Actions: was connected by process iexplore[.]exe
- **10:40:01 -** Asset/Incident Responder: device Vic **-** Actions: was communicated with by ip 185[.]199[.]109[.]133
- **10:40:01 -** Asset/Incident Responder: device Vic **-** Actions: was communicated with by url hXXp://attacker[.]ihatemikesimone[.]com:8888/
- **10:40:01 -** Asset/Incident Responder: device Vic **-** Actions: was connected by process svchost[.]exe
- **10:40:01 -** Asset/Incident Responder: device Vic **-** Actions: was connected by process mshta[.]exe
- **10:40:01 -** Asset/Incident Responder: device Vic **-** Actions: was communicated with by ip 198[.]19[.]255[.]146
- **10:40:01 -** Asset/Incident Responder: device Vic **-** Actions: was connected to ip 198[.]18[.]133[.]150
- **10:40:01 -** Asset/Incident Responder: device Vic **-** Actions: was communicated with by url hXXp://198[.]18[.]133[.]150:8000/attack[.]hta
- **10:40:01 -** Asset/Incident Responder: device Vic **-** Actions: was connected by process powershell[.]exe (3 times)
- **10:40:01 -** Asset/Incident Responder: device Vic **-** Actions: was communicated with by url hXXps://download[.]sysinternals[.]com/files/PSTools[.]zip/
- **10:40:01 -** Asset/Incident Responder: device Vic **-** Actions: was observed on by process svchost[.]exe
- **10:40:01 -** Asset/Incident Responder: device Vic **-** Actions: executed process svchost[.]exe (2 times)
- **10:40:01 -** Asset/Incident Responder: device Vic **-** Actions: communicated with process powershell[.]exe (2 times)
- **10:40:01 -** Asset/Incident Responder: device Vic **-** Actions: executed process services[.]exe
- **10:40:01 -** Asset/Incident Responder: device Vic **-** Actions: executed process powershell[.]exe (3

times)

- **10:40:01 -** Asset/Incident Responder: device Vic **-** Actions: used by user vic
- **10:40:01 -** Asset/Incident Responder: device Vic **-** Actions: accessed process svchost[.]exe
- **10:40:01 -** Asset/Incident Responder: device Vic **-** Actions: communicated with process nslookup[.]exe (6 times)
- **10:40:01 -** Asset/Incident Responder: device Vic **-** Actions: communicated with process svchost[.]exe
- **10:40:01 -** Asset/Incident Responder: device Vic **-** Actions: communicated with process mshta[.]exe
- **10:40:01 -** Asset/Incident Responder: device Vic **-** Actions: connected to ip 198[.]18[.]133[.]150
- **10:40:01 -** Asset/Incident Responder: device Vic **-** Actions: executed process powershell[.]exe
- **10:40:01 -** Asset/Incident Responder: device Vic **-** Actions: executed process svchost[.]exe
- **10:40:01 -** Asset/Incident Responder: device Vic **-** Actions: connected to url hXXp://attacker[.]ihatemikesimone[.]com:8888/
- **10:40:01 -** Asset/Incident Responder: device Vic **-** Actions: connected to ip 198[.]19[.]255[.]146
- **10:40:01 -** Asset/Incident Responder: device Vic **-** Actions: connected to url hXXp://198[.]18[.]133[.]150:8000/attack[.]hta
- **10:40:01 -** Asset/Incident Responder: device Vic **-** Actions: connected to url hXXps://download[.]sysinternals[.]com/files/PSTools[.]zip/
- **10:40:01 -** Asset/Incident Responder: device Vic **-** Actions: executed process nslookup[.]exe (6 times)
- **10:40:01 -** Asset/Incident Responder: device Vic **-** Actions: communicated with device Vic
- **10:40:01 -** Asset/Incident Responder: device Vic **-** Actions: connected to url hXXp://198[.]18[.]133[.]150:8888/
- **10:40:01 -** Asset/Incident Responder: device Vic **-** Actions: communicated with process powershell[.]exe (2 times)
- **10:40:01 -** Asset/Incident Responder: device Vic **-** Actions: executed process powershell[.]exe
- **10:40:01 -** Asset/Incident Responder: device Vic **-** Actions: executed process svchost[.]exe
- **10:40:01 -** Asset/Incident Responder: device Vic **-** Actions: executed process mshta[.]exe (4 times)
- **10:40:01 -** Asset/Incident Responder: device Vic **-** Actions: executed process iexplore[.]exe
- **10:40:01 -** Asset/Incident Responder: device Vic **-** Actions: accessed files cryptdll[.]dll, samlib[.]dll, WinSCard.dll and 2 more
- **10:40:01 -** Asset/Incident Responder: device Vic **-** Actions: executed process powershell[.]exe (12 times)
- **10:40:01 -** Asset/Incident Responder: user vic **-** Actions: accessed device Vic
- **10:40:01 -** Asset/Incident Responder: user vic **-** Actions: executed process iexplore[.]exe
- **10:40:01 -** Asset/Incident Responder: user XDRI/vic **-** Actions: accessed device Vic
- **10:40:01 -** Asset/Incident Responder: user XDRI/vic **-** Actions: assigned to device Vic
- **10:40:01 -** Asset/Incident Responder: device dc01[.]xdri[.]local **-** Actions: was communicated with by ip 198[.]18[.]133[.]150
- **10:40:01 -** Asset/Incident Responder: device dc01[.]xdri[.]local **-** Actions: communicated with

device Vic

- **10:40:01 -** Asset/Incident Responder: device dc01[.]xdri[.]local **-** Actions: connected to device Vic
- **10:40:01 -** Asset/Incident Responder: device dc01[.]xdri[.]local **-** Actions: accessed device Vic
- **10:40:01 -** Asset/Incident Responder: device dc01[.]xdri[.]local **-** Actions: connected to ip 198[.]18[.]133[.]150
- **10:40:01 -** Asset/Incident Responder: device dc01[.]xdri[.]local **-** Actions: executed process iexplore[.]exe

September 22, 2025

- **04:02:15 -** Asset/Incident Responder: user NT AUTHORITY/SYSTEM **-** Actions: executed process svchost[.]exe
- **04:02:15 -** Asset/Incident Responder: user vic **-** Actions: executed process svchost[.]exe
- **04:02:15 -** Asset/Incident Responder: user XDRI.LOCAL/vic **-** Actions: executed process svchost[.]exe
- **04:02:15 -** Asset/Incident Responder: user XDRI/vic **-** Actions: executed process svchost[.]exe
- **04:02:15 -** Asset/Incident Responder: device dc01[.]xdri[.]local **-** Actions: was connected by process svchost[.]exe
- **04:02:15 -** Asset/Incident Responder: device dc01[.]xdri[.]local **-** Actions: was observed on by process svchost[.]exe
- **04:02:15 -** Asset/Incident Responder: device dc01[.]xdri[.]local **-** Actions: executed process svchost[.]exe
- **04:02:15 -** Asset/Incident Responder: device dc01[.]xdri[.]local **-** Actions: accessed process svchost[.]exe
- **04:02:19 -** Asset/Incident Responder: user SYSTEM **-** Actions: was used by process svchost[.]exe
- **04:02:19 -** Asset/Incident Responder: user SYSTEM **-** Actions: executed process svchost[.]exe
- **04:02:19 -** Asset/Incident Responder: user vic **-** Actions: was used by process svchost[.]exe
- **04:02:19 -** Asset/Incident Responder: user vic **-** Actions: was used by process mshta[.]exe
- **04:02:19 -** Asset/Incident Responder: user vic **-** Actions: was used by process powershell[.]exe (2 times)
- **04:02:19 -** Asset/Incident Responder: user vic **-** Actions: executed process mshta[.]exe
- **04:02:19 -** Asset/Incident Responder: user vic **-** Actions: executed process powershell[.]exe (4 times)
- **04:02:19 -** Asset/Incident Responder: user vic **-** Actions: executed process svchost[.]exe
- **04:02:19 -** Asset/Incident Responder: user XDRI.LOCAL/vic **-** Actions: executed process powershell[.]exe (5 times)
- **04:02:19 -** Asset/Incident Responder: user XDRI/vic **-** Actions: executed process powershell[.]exe (3 times)
- **04:02:19 -** Asset/Incident Responder: user XDRI/vic **-** Actions: executed process WMIC.exe
- **04:02:19 -** Asset/Incident Responder: user XDRI/vic **-** Actions: executed process netsh[.]exe

- **04:02:19 -** Asset/Incident Responder: user XDRI/vic **-** Actions: executed process powershell[.]exe
- **04:02:19 -** Asset/Incident Responder: user XDRI/vic **-** Actions: assigned to device dc01[.]xdri[.]local
- **04:02:19 -** Asset/Incident Responder: user XDRI/vic **-** Actions: executed process powershell[.]exe
- **04:02:19 -** Asset/Incident Responder: user XDRI/vic **-** Actions: executed process ARP.EXE
- **04:02:19 -** Asset/Incident Responder: user XDRI/vic **-** Actions: executed process cmd[.]exe
- **04:02:19 -** Asset/Incident Responder: user XDRI/vic **-** Actions: executed process wsmprovhost[.]exe
- **04:02:19 -** Asset/Incident Responder: user XDRI/vic **-** Actions: executed process gpresult[.]exe
- **04:02:19 -** Asset/Incident Responder: user XDRI/vic **-** Actions: executed process mshta[.]exe
- **04:02:19 -** Asset/Incident Responder: user XDRI/vic **-** Actions: executed process tasklist[.]exe
- **04:02:19 -** Asset/Incident Responder: user XDRI/vic **-** Actions: executed process nbtstat[.]exe
- **04:02:19 -** Asset/Incident Responder: user XDRI/vic **-** Actions: executed process explorer[.]exe
- **04:02:19 -** Asset/Incident Responder: device dc01[.]xdri[.]local **-** Actions: was communicated with by url hXXp://198[.]18[.]133[.]150:8888/
- **04:02:19 -** Asset/Incident Responder: device dc01[.]xdri[.]local **-** Actions: was used by process mshta[.]exe
- **04:02:19 -** Asset/Incident Responder: device dc01[.]xdri[.]local **-** Actions: was connected by process powershell[.]exe
- **04:02:19 -** Asset/Incident Responder: device dc01[.]xdri[.]local **-** Actions: was used by process powershell[.]exe (2 times)
- **04:02:19 -** Asset/Incident Responder: device dc01[.]xdri[.]local **-** Actions: was observed on by process svchost[.]exe
- **04:02:19 -** Asset/Incident Responder: device dc01[.]xdri[.]local **-** Actions: was used by process svchost[.]exe
- **04:02:19 -** Asset/Incident Responder: device dc01[.]xdri[.]local **-** Actions: executed process powershell[.]exe (4 times)
- **04:02:19 -** Asset/Incident Responder: device dc01[.]xdri[.]local **-** Actions: executed process svchost[.]exe (2 times)
- **04:02:19 -** Asset/Incident Responder: device dc01[.]xdri[.]local **-** Actions: executed process mshta[.]exe
- **04:02:19 -** Asset/Incident Responder: device dc01[.]xdri[.]local **-** Actions: accessed process svchost[.]exe
- **04:02:19 -** Asset/Incident Responder: device dc01[.]xdri[.]local **-** Actions: connected to url hXXp://198[.]18[.]133[.]150:8888/

September 24, 2025

- **09:33:58 -** Asset/Incident Responder: device dc01[.]xdri[.]local **-** Actions: was communicated with by url hXXps://download[.]sysinternals[.]com/files/PSTools[.]zip/

- **09:33:58 -** Asset/Incident Responder: device dc01[.]xdri[.]local **-** Actions: connected to url hXXps://download[.]sysinternals[.]com/files/PSTools[.]zip/
- **09:39:12 -** Asset/Incident Responder: user XDRI/administrator **-** Actions: accessed device dc01[.]xdri[.]local
- **09:39:12 -** Asset/Incident Responder: user NT AUTHORITY/SYSTEM **-** Actions: assigned to device dc01[.]xdri[.]local
- **09:39:12 -** Asset/Incident Responder: user NT AUTHORITY/SYSTEM **-** Actions: executed process lsass[.]exe
- **09:39:12 -** Asset/Incident Responder: user NETWORK SERVICE **-** Actions: accessed device dc01[.]xdri[.]local
- **09:39:12 -** Asset/Incident Responder: user NETWORK SERVICE **-** Actions: executed process WmiPrvSE.exe
- **09:39:12 -** Asset/Incident Responder: user vic **-** Actions: accessed device dc01[.]xdri[.]local
- **09:39:12 -** Asset/Incident Responder: user XDRI.LOCAL/vic **-** Actions: executed process ARP.EXE
- **09:39:12 -** Asset/Incident Responder: user XDRI.LOCAL/vic **-** Actions: executed process tasklist[.]exe
- **09:39:12 -** Asset/Incident Responder: user XDRI.LOCAL/vic **-** Actions: assigned to device dc01[.]xdri[.]local
- **09:39:12 -** Asset/Incident Responder: user XDRI.LOCAL/vic **-** Actions: executed process gpresult[.]exe
- **09:39:12 -** Asset/Incident Responder: user XDRI.LOCAL/vic **-** Actions: executed process WMIC.exe
- **09:39:12 -** Asset/Incident Responder: user XDRI.LOCAL/vic **-** Actions: executed process nbtstat[.]exe
- **09:39:12 -** Asset/Incident Responder: user XDRI.LOCAL/vic **-** Actions: executed process netsh[.]exe
- **09:39:12 -** Asset/Incident Responder: device dc01[.]xdri[.]local **-** Actions: was communicated with by url hXXps://raw[.]githubusercontent[.]com/PowerShellMafia/PowerSploit/4c7a2016fc7931cd37273c5d8e17b16d959867b3/Exfiltration/Invoke-Mimikatz[.]ps1/
- **09:39:12 -** Asset/Incident Responder: device dc01[.]xdri[.]local **-** Actions: was connected by process WmiPrvSE.exe
- **09:39:12 -** Asset/Incident Responder: device dc01[.]xdri[.]local **-** Actions: was observed on by file wifi[.]ps1
- **09:39:12 -** Asset/Incident Responder: device dc01[.]xdri[.]local **-** Actions: was communicated with by ips 192[.]168[.]6[.]10, 192[.]168[.]6[.]12, 198[.]18[.]6[.]5 and 2 more
- **09:39:12 -** Asset/Incident Responder: device dc01[.]xdri[.]local **-** Actions: was communicated with by swc device id 405
- **09:39:12 -** Asset/Incident Responder: device dc01[.]xdri[.]local **-** Actions: was used by process nslookup[.]exe (6 times)
- **09:39:12 -** Asset/Incident Responder: device dc01[.]xdri[.]local **-** Actions: was used by process powershell[.]exe (2 times)

- **09:39:12 -** Asset/Incident Responder: device dc01[.]xdri[.]local **-** Actions: connected to ips 192[.]168[.]6[.]10, 192[.]168[.]6[.]12, 198[.]18[.]6[.]5 and 2 more
- **09:39:12 -** Asset/Incident Responder: device dc01[.]xdri[.]local **-** Actions: connected to ips 239[.]255[.]255[.]250, 224[.]0[.]0[.]251, 224[.]0[.]0[.]22 and 1 more
- **09:39:12 -** Asset/Incident Responder: device dc01[.]xdri[.]local **-** Actions: executed process mshta[.]exe
- **09:39:12 -** Asset/Incident Responder: device dc01[.]xdri[.]local **-** Actions: executed process WMIC.exe
- **09:39:12 -** Asset/Incident Responder: device dc01[.]xdri[.]local **-** Actions: connected to device dc01[.]xdri[.]local
- **09:39:12 -** Asset/Incident Responder: device dc01[.]xdri[.]local **-** Actions: executed processes nbtstat[.]exe, netsh[.]exe, tasklist[.]exe and 3 more
- **09:39:12 -** Asset/Incident Responder: device dc01[.]xdri[.]local **-** Actions: executed process WmiPrvSE.exe
- **09:39:12 -** Asset/Incident Responder: device dc01[.]xdri[.]local **-** Actions: executed process powershell[.]exe (15 times)
- **09:39:12 -** Asset/Incident Responder: device dc01[.]xdri[.]local **-** Actions: executed process wsmprovhost[.]exe (2 times)
- **09:39:12 -** Asset/Incident Responder: device dc01[.]xdri[.]local **-** Actions: accessed device dc01[.]xdri[.]local
- **09:39:12 -** Asset/Incident Responder: device dc01[.]xdri[.]local **-** Actions: executed process powershell[.]exe
- **09:39:12 -** Asset/Incident Responder: device dc01[.]xdri[.]local **-** Actions: connected to url hXXps://raw[.]githubusercontent[.]com/PowerShellMafia/PowerSploit/4c7a2016fc7931cd37273c5d8e17b16d959867b3/Exfiltration/Invoke-Mimikatz[.]ps1/
- **09:39:12 -** Asset/Incident Responder: device dc01[.]xdri[.]local **-** Actions: executed process nslookup[.]exe (6 times)
- **09:39:12 -** Asset/Incident Responder: device dc01[.]xdri[.]local **-** Actions: executed process wininit[.]exe
- **09:39:12 -** Asset/Incident Responder: device dc01[.]xdri[.]local **-** Actions: used by user vic
- **09:39:12 -** Asset/Incident Responder: device dc01[.]xdri[.]local **-** Actions: executed processes powershell[.]exe, conhost[.]exe
- **09:39:12 -** Asset/Incident Responder: device dc01[.]xdri[.]local **-** Actions: connected to ip 192[.]168[.]6[.]135
- **09:39:12 -** Asset/Incident Responder: device dc01[.]xdri[.]local **-** Actions: executed process WmiPrvSE.exe (2 times)
- **09:39:12 -** Asset/Incident Responder: device dc01[.]xdri[.]local **-** Actions: executed process lsass[.]exe

September 25, 2025

- **08:52:25 -** Asset/Incident Responder: user vic **-** Actions: was used by processes nbtstat[.]exe, netsh[.]exe, tasklist[.]exe and 3 more
- **08:52:25 -** Asset/Incident Responder: user vic **-** Actions: was used by process powershell[.]exe (5 times)
- **08:52:25 -** Asset/Incident Responder: user vic **-** Actions: was used by process nslookup[.]exe (6 times)
- **08:52:25 -** Asset/Incident Responder: user vic **-** Actions: was used by process wsmprovhost[.]exe
- **08:52:25 -** Asset/Incident Responder: user vic **-** Actions: was used by process mshta[.]exe
- **08:52:25 -** Asset/Incident Responder: user vic **-** Actions: was used by process powershell[.]exe
- **08:52:25 -** Asset/Incident Responder: user vic **-** Actions: was used by processes powershell[.]exe, conhost[.]exe
- **08:52:25 -** Asset/Incident Responder: user vic **-** Actions: was used by process WMIC.exe
- **08:52:25 -** Asset/Incident Responder: user vic **-** Actions: executed processes powershell[.]exe, conhost[.]exe
- **08:52:25 -** Asset/Incident Responder: user vic **-** Actions: executed process mshta[.]exe
- **08:52:25 -** Asset/Incident Responder: user vic **-** Actions: sent email message Fw: These folks are keen - who is hpurple? - will this ever get through? !!!!
- **08:52:25 -** Asset/Incident Responder: user vic **-** Actions: executed process powershell[.]exe (14 times)
- **08:52:25 -** Asset/Incident Responder: user vic **-** Actions: executed processes nbtstat[.]exe, netsh[.]exe, tasklist[.]exe and 3 more
- **08:52:25 -** Asset/Incident Responder: user vic **-** Actions: executed process wsmprovhost[.]exe
- **08:52:25 -** Asset/Incident Responder: user vic **-** Actions: executed process powershell[.]exe
- **08:52:25 -** Asset/Incident Responder: user vic **-** Actions: executed process WMIC.exe
- **08:52:25 -** Asset/Incident Responder: user vic **-** Actions: executed process nslookup[.]exe (6 times)

September 27, 2025

- **10:49:04 -** Asset/Incident Responder: user NETWORK SERVICE **-** Actions: was used by process WmiPrvSE.exe
- **10:49:04 -** Asset/Incident Responder: user NETWORK SERVICE **-** Actions: executed process WmiPrvSE.exe (2 times)

September 28, 2025

- **04:20:55 -** Asset/Incident Responder: user SYSTEM **-** Actions: was used by process lsass[.]exe
- **04:20:55 -** Asset/Incident Responder: user SYSTEM **-** Actions: executed process lsass[.]exe
- **04:21:04 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: incident promoted
- **04:21:06 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: techniques

changed

- **04:21:06 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: modified
- **04:21:08 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: [Response Task] Analysis: Recent Suspicious Events
- **04:21:08 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: [Response Task] Analysis: Endpoints with Potentially Malicious Files
- **04:21:08 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: [Response Task] Analysis: IPs, Domains, or URLs Involved in the Incident
- **04:21:08 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: modified
- **04:22:13 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: short description changed
- **04:22:13 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: meta added
- **04:22:13 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: modified
- **04:22:13 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: description changed
- **04:26:05 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: modified
- **04:26:05 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: external references changed
- **04:26:07 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: tactics changed
- **04:26:07 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: detection sources changed
- **04:26:07 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: modified
- **04:26:07 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: scores changed
- **04:26:07 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: techniques changed
- **04:26:07 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: modified
- **04:26:08 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: [Response Task] Analysis: Recent Suspicious Events
- **04:26:08 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: [Response Task] Analysis: Endpoints with Potentially Malicious Files
- **04:26:08 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: [Response Task] Analysis: IPs, Domains, or URLs Involved in the Incident
- **04:26:26 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: title changed
- **04:26:26 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: description changed
- **04:26:26 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: modified
- **04:26:26 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: short description changed
- **04:36:00 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: external references changed
- **04:36:00 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: modified
- **04:42:07 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: modified

- **04:42:07 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: external references changed
- **04:42:08 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: modified
- **04:42:08 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: techniques changed
- **04:42:08 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: detection sources changed
- **04:42:08 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: tactics changed
- **04:42:08 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: scores changed
- **04:42:08 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: [Response Task] Analysis: Recent Suspicious Events
- **04:42:08 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: [Response Task] Analysis: Endpoints with Potentially Malicious Files
- **04:42:08 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: [Response Task] Analysis: IPs, Domains, or URLs Involved in the Incident
- **04:42:09 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: modified
- **04:44:55 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: external references changed
- **04:44:55 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: modified
- **04:45:31 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: modified
- **04:45:31 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: external references changed
- **04:45:32 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: modified
- **04:45:32 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: scores changed
- **04:45:32 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: tactics changed
- **04:45:32 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: techniques changed
- **04:45:33 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: [Response Task] Analysis: Endpoints with Potentially Malicious Files
- **04:45:33 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: techniques changed
- **04:45:33 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: scores changed
- **04:45:33 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: modified
- **04:45:33 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: tactics changed
- **04:45:40 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: modified
- **04:45:40 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: external references changed
- **04:47:37 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: modified
- **04:47:37 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: external references changed
- **04:47:38 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: techniques changed

- **04:47:38 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: modified
- **04:47:38 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: tactics changed
- **04:47:38 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: tactics changed
- **04:47:38 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: modified
- **04:47:38 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: techniques changed
- **04:51:01 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: modified
- **04:51:01 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: external references changed
- **04:51:03 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: modified
- **04:51:03 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: techniques changed
- **04:51:03 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: modified
- **04:51:04 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: [Response Task] Analysis: Recent Suspicious Events
- **04:51:04 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: [Response Task] Analysis: Endpoints with Potentially Malicious Files
- **04:51:04 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: [Response Task] Analysis: IPs, Domains, or URLs Involved in the Incident
- **04:53:19 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: external references changed
- **04:53:19 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: modified
- **04:53:20 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: modified
- **04:53:20 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: techniques changed
- **04:53:20 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: [Response Task] Analysis: Recent Suspicious Events
- **04:53:20 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: [Response Task] Analysis: Endpoints with Potentially Malicious Files
- **04:53:20 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: [Response Task] Analysis: IPs, Domains, or URLs Involved in the Incident
- **04:53:20 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: techniques changed
- **04:53:20 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: modified
- **04:53:55 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: external references changed
- **04:53:55 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: modified
- **04:53:56 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: detection sources changed
- **04:53:56 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: techniques changed
- **04:53:56 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: tactics changed

- **04:53:56 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: modified
- **04:53:57 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: modified
- **04:53:57 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: techniques changed
- **04:53:57 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: tactics changed
- **04:53:57 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: detection sources changed
- **04:55:07 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: modified
- **04:55:07 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: external references changed
- **04:55:08 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: techniques changed
- **04:55:08 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: modified
- **04:55:09 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: techniques changed
- **04:55:09 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: modified
- **04:55:50 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: modified
- **04:55:50 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: external references changed
- **04:55:51 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: [Response Task] Analysis: Recent Suspicious Events
- **04:55:51 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: [Response Task] Analysis: Endpoints with Potentially Malicious Files
- **05:00:48 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: modified
- **05:00:48 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: external references changed
- **05:00:49 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: modified
- **05:00:49 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: techniques changed
- **05:00:49 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: modified
- **05:00:49 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: techniques changed
- **05:00:50 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: [Response Task] Analysis: Endpoints with Potentially Malicious Files
- **05:00:50 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: [Response Task] Analysis: IPs, Domains, or URLs Involved in the Incident
- **05:06:10 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: external references changed
- **05:06:10 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: modified
- **05:06:12 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: modified
- **05:06:12 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: techniques changed

- **05:06:12 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: modified
- **05:06:12 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: techniques changed
- **05:06:13 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: [Response Task] Analysis: Endpoints with Potentially Malicious Files
- **05:08:19 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: external references changed
- **05:08:19 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: modified
- **05:08:20 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: [Response Task] Analysis: Endpoints with Potentially Malicious Files
- **05:10:58 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: modified
- **05:10:58 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: external references changed
- **05:11:00 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: [Response Task] Analysis: Endpoints with Potentially Malicious Files
- **05:11:00 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: [Response Task] Analysis: IPs, Domains, or URLs Involved in the Incident
- **05:13:45 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: modified
- **05:13:45 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: external references changed
- **05:13:46 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: [Response Task] Analysis: Recent Suspicious Events
- **05:13:46 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: [Response Task] Analysis: IPs, Domains, or URLs Involved in the Incident
- **05:16:06 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: external references changed
- **05:16:06 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: modified
- **05:16:08 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: [Response Task] Analysis: Recent Suspicious Events
- **05:16:08 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: [Response Task] Analysis: Endpoints with Potentially Malicious Files
- **05:16:08 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: [Response Task] Analysis: IPs, Domains, or URLs Involved in the Incident
- **05:20:35 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: external references changed
- **05:20:35 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: modified
- **05:21:00 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: modified
- **05:21:00 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: external references changed
- **05:21:02 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: [Response Task] Analysis: Recent Suspicious Events
- **05:21:02 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: [Response Task]

Analysis: IPs, Domains, or URLs Involved in the Incident

- **05:22:11 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: modified
- **05:22:11 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: external references changed
- **05:22:13 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: [Response Task] Analysis: Recent Suspicious Events
- **05:33:57 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: modified
- **05:33:57 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: external references changed
- **06:32:24 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: modified
- **06:32:24 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: external references changed
- **06:32:26 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: [Response Task] Analysis: Endpoints with Potentially Malicious Files
- **06:34:00 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: external references changed
- **06:34:00 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: modified
- **06:41:26 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: external references changed
- **06:41:26 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: modified
- **10:27:26 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: title changed
- **10:27:26 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: description changed
- **10:27:26 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: modified
- **10:27:26 -** Asset/Incident Responder: Cisco Security Workshop - RIR **-** Actions: short description changed

September 29, 2025

- **11:55:42 -** Incident Responder: Sam Sanderson **-** Actions: status changed
- **11:55:42 -** Incident Responder: Sam Sanderson **-** Actions: incident time changed
- **11:55:42 -** Incident Responder: Sam Sanderson **-** Actions: modified
- **11:55:43 -** Incident Responder: Sam Sanderson **-** Actions: assignees added
- **11:55:43 -** Incident Responder: Sam Sanderson **-** Actions: modified