**Command & Control**

| **Ref #** | **Phase** | **Category** | **Attack Variation** | **Outcome** | **Outcome Details** | **Outcome Notes** | **Detection / Prevention Tools** | **Tags** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| C2-1 | Command & Control | Application Layer Protocol | T1071 - Command & Control - HTTP(S) Slow Beaconing activity | Detected | Medium Severity |  | Splunk |  |
| C2-2 | Command & Control | Data Encoding | T1132 - Base64 Encoded data. | Detected | To Be Determined |  |  | Data Source is unknown |
| C2-3 | Command & Control | Connection Proxy | T1090 - Connection Proxy | Detected | To Be Determined |  | Splunk | Data Source is unknown |
| C2-4 | Command & Control | Uncommonly Used Port | T1065 - Testing usage of uncommonly used port | Blocked | Alert Not Triggered |  |  | Data Source is unknown |
| C2-5 | Command & Control | Commonly Used Port | Cobalt Strike Default Beacon HTTPS payload over tcp/443 | Detected | To Be Determined |  | Splunk | IsLogged  Sysmon  Mandiant  High Priority |
| C2-6 | Command & Control | Custom Command and Control Protocol | Cobalt Strike Custom Beacon HTTP payload over tcp/80 | Detected | To Be Determined |  | Splunk | IsLogged  Sysmon  Mandiant  High Priority |
| C2-7 | Command & Control | Commonly Used Port | Beacon DNS over udp/53 (A) | Detected | High Severity |  | Splunk | Mandiant |
| C2-8 | Command & Control | C2 channel | Cobalt Strike Default Beacon SMB over tcp/445 | Not Detected | Activity Logged | See FireEye IOCs for this |  | Needs work  IsLogged |
| C2-9 | Command & Control | Commonly Used Port | Beacon DNS over udp/53 (TXT) | Detected | High Severity |  | Splunk | Mandiant |

**Privilege Escalation**

| **Ref #** | **Phase** | **Category** | **Attack Variation** | **Outcome** | **Outcome Details** | **Outcome Notes** | **Detection / Prevention Tools** | **Tags** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| PRIV-ESC-1 | Privilege Escalation | AppInit DLLs | T1103 - Install AppInit Shim | Not Detected | No Activity Logged |  |  | NotLogged  Sysmon |
| PRIV-ESC-2 | Privilege Escalation | Access Token Manipulation | RunAs execution | Detected | To Be Determined |  |  |  |
| PRIV-ESC-3 | Privilege Escalation | Dynamic-link Library Injection | Ricoh Printer exploit | Detected | To Be Determined |  | Splunk | Testing Completed  Sysmon |
| PRIV-ESC-4 | Privilege Escalation | Exploitation for Privilege Escalation | T1068 - Privilege Escalation - NTLM relay from Domain Controller | Detected | Medium Severity | The objective of this use is to detect what a Kerberos TGT request for the computer account of any BOCAD domain controller is requested from an IP address that is not a domain controller | Splunk |  |
| PRIV-ESC-5 | Privilege Escalation | Access Token Manipulation | T1134 - Privilege Escalation - RunAs logon account mismatch | Detected | Medium Severity | The objective of this use case is to alert on a condition where the 'runas' account doesn't match or is not owned by the user initating the process/runas | Splunk |  |
| PRIV-ESC-6 | Privilege Escalation | Image File Execution Options Injection | T1183 - IFEO Add Debugger | Not Detected | No Activity Logged |  |  | NotLogged  Sysmon |
| PRIV-ESC-7 | Privilege Escalation | Image File Execution Options Injection | T1183 - IFEO Global Flags | Not Detected | Activity Logged To Be Determined |  |  | Sysmon |
| PRIV-ESC-8 | Privilege Escalation | Bypass User Account Control | T1088 - Bypass UAC using Event Viewer | Blocked | Alert Triggered To Be Determined |  |  | Sysmon |
| PRIV-ESC-9 | Privilege Escalation | Exploitation for Privilege Escalation | Suspect child of Consent.exe | Not Detected | Activity Logged |  |  | IsLogged |
| PRIV-ESC-10 | Privilege Escalation | Bypass User Account Control | T1088 - Bypass UAC using Fodhelper | Blocked | Alert Triggered To Be Determined |  |  | Sysmon |
| PRIV-ESC-11 | Privilege Escalation | Bypass User Account Control | T1088 - Bypass UAC using Fodhelper - PowerShell | Blocked | Alert Triggered To Be Determined |  | Windows Defender (Standard) | Sysmon |
| PRIV-ESC-12 | Privilege Escalation | Application Shimming | T1138 - Application Shim Installation | Not Detected | Activity Logged |  |  | IsLogged |
| PRIV-ESC-13 | Privilege Escalation | Windows Command Shell | CMD use of Name Pipe | Not Detected | Activity Logged |  |  | IsLogged |
| PRIV-ESC-14 | Privilege Escalation | Bypass User Account Control | T1088 - Bypass UAC using Event Viewer - PowerShell | Blocked | Alert Triggered To Be Determined |  |  | Sysmon |
| PRIV-ESC-15 | Privilege Escalation | Exploitation for Privilege Escalation | T1068 - Privilege Escalation - Suspicious .sys driver executed | Detected | Medium Severity | The objective of this use case is to alert when a driver with .sys extension is created and or downloaded into a workstation in a user writeable directory or in a directory that is unusual for drivers to reside other than C:\Windows\System32\Drivers; C:\WINDOWS\system32\DriverStore\FileRepository. | Splunk |  |
| PRIV-ESC-16 | Privilege Escalation | Exploitation for Privilege Escalation | T1068 - Privilege Escalation - Use of PrintNightmare SystemNightmare | Detected | Medium Severity |  | Splunk |  |
| PRIV-ESC-17 | Privilege Escalation | Exploitation for Privilege Escalation | Privilege Escalation Checks | Not Detected | Activity Logged To Be Determined |  |  | Sysmon |

**Execution**

| **Ref #** | **Phase** | **Category** | **Attack Variation** | **Outcome** | **Outcome Details** | **Outcome Notes** | **Detection / Prevention Tools** | **Tags** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| EXE-1 | Execution | Mshta | Atomic MSHTA test | Detected | High Severity |  | Splunk | Needs work |
| EXE-2 | Execution | User Execution | T1204 - Execution - AppLocker bypass via folder exclusion | Detected | Medium Severity | This use case looks for any executable whose path begins with those excluded in the AppLocker configuration but are new from what the baseline has been for the last 90 days. | Splunk |  |
| EXE-3 | Execution | User Execution | T1204 - Execution - Potentially Malicious Script Downloaded from Internet on Host | Detected | Medium Severity | The objective of this use case is to alert in the event a malicious scripting file is downloaded via the internet in a user writable directory such as: C:\ProgramData ; C:\users ; C:\temp ; Local\Temp ; \Start Menu\ | Splunk |  |
| EXE-4 | Execution | User Execution | T1204 - Execution - Windows scripting host wrote a suspicious .dll | Detected | Medium Severity | This use case looks for either wscript.exe or cscript.exe creating a .dll file outside of trusted folders. | Splunk |  |
| EXE-5 | Execution | User Execution | T1204 - Execution - Potentially malicious DLL written to disk | Detected | To Be Determined | The object of this use case is to create a notable event for any process that writes fewer than 3 DLLs to disk within a 5 minute window. This behvaiour is indicative of either an initial access mechanism or one of persistence. | Splunk |  |
| EXE-6 | Execution | Signed Binary Proxy Execution | Invoke RemoteFXvGPUDisablement Command | Detected | To Be Determined |  |  |  |
| IMPACT-7 | Impact | File Deletion | wbadmin.exe execution (ransomware) | Detected | To Be Determined |  | Splunk | IsLogged |
| EXE-8 | Execution | PowerShell | PowerShell loading & executing a .dll | Not Detected | Activity Logged |  |  | Sysmon |
| EXE-9 | Execution | Signed Binary Proxy Execution | MakeCab.exe as a lolbin | Not Detected | Activity Logged |  |  | Needs work  IsLogged |
| EXE-10 | Execution | Trusted Developer Utilities Proxy Execution | PowerShell MSbuild (MSBuild w/o MSBuild) | Detected | To Be Determined |  | Splunk | Sysmon  Todd |
| EXE-11 | Execution | Compiled HTML File | Compiled HTML file | Detected | To Be Determined |  |  | IsLogged |
| EXE-12 | Execution | Windows Command Shell | CMD odd cmd line arguments | Not Detected | Activity Logged |  |  | IsLogged |
| EXE-13 | Execution | Signed Binary Proxy Execution | Rundll32 executing an .hta file | Detected | To Be Determined |  | Splunk | Needs work  IsLogged |
| EXE-14 | Execution | Signed Binary Proxy Execution | Rundll32 shdocvw.dll, OpenURL | Detected | To Be Determined |  | Splunk | Needs work  IsLogged |
| EXE-15 | Execution | Signed Binary Proxy Execution | Rundll32 executing an .hta file CLONE | Detected | To Be Determined |  | Splunk |  |
| EXE-16 | Execution | Signed Binary Proxy Execution | RunDll32 DllRegisterServer mount point | Detected | To Be Determined |  | Splunk | Needs work  IsLogged |
| EXE-17 | Execution | Signed Binary Proxy Execution | RunDll32 url.dll fileprotocolhandler | Detected | To Be Determined |  |  | Needs work  IsLogged |
| EXE-18 | Execution | Internal Spearphishing | Outlook executing a OTM file | Not Detected | Activity Logged |  |  | IsLogged |
| IMPACT-19 | Impact | File Deletion | bcdedit.exe execution (ransomware) | Detected | To Be Determined |  | Splunk | IsLogged |
| EXE-20 | Execution | Mshta | Atomic test harness - MSHTA tests | Detected | Medium Severity |  | Splunk | Needs work |
| EXE-21 | Execution | PowerShell | PowerShell Start-Process cmdlet | Not Detected | Activity Logged |  |  | Data onboarding req |
| EXE-22 | Execution | Trusted Developer Utilities Proxy Execution | MSBuild without MSBuild | Detected | To Be Determined |  |  | Testing Completed  Sysmon  High Priority |
| EXE-23 | Execution | Command and Scripting Interpreter | T1059 - Execution - Rare wscript execution on workstation | Detected | High Severity | The objective of this use case is to detect the execution of wscript.exe on workstations by regular or admin users where the command line points to a user writtable file location and the command line does not contain either the /b or /e operators. | Splunk |  |
| EXE-24 | Execution | PowerShell | T1086 - Powershell invoke mshta.exe download | Detected | To Be Determined |  | Splunk | IsLogged |
| EXE-25 | Execution | Service Execution | Service Execution | Detected | To Be Determined |  | Splunk | Needs work |
| EXE-26 | Execution | Command and Scripting Interpreter | Malicious CScript Execution | Detected | To Be Determined |  | Splunk | Needs work |
| EXE-27 | Execution | User Execution | Malicious Archive File | Detected | To Be Determined |  |  | Todd |
| EXE-28 | Execution | Windows Management Instrumentation | wmic.exe process creation | Detected | High Severity |  | Splunk |  |
| EXE-29 | Execution | Signed Binary Proxy Execution | LOLBAS - Downloaders/Stagers | Detected | High Severity |  |  | Needs work |
| EXE-30 | Execution | Windows Management Instrumentation | Invoke-WMIMethod | Not Detected | Activity Logged To Be Determined |  |  | Data onboarding req  IsLogged  Todd |
| EXE-31 | Execution | Spearphishing Attachment | Various Maldoc samples | Not Detected | Activity Logged To Be Determined |  |  | Sysmon |
| EXE-32 | Execution | Spearphishing Attachment | More Malcious Maldocs - COM | Not Detected | Activity Logged To Be Determined |  |  | Sysmon |
| EXE-33 | Execution | PowerShell | PowerShell PSReflect | Not Detected | Activity Logged To Be Determined | May require EID 800 filtering |  | Todd |
| EXE-34 | Execution | PowerShell | PowerShell Add-Type | Not Detected | Activity Logged To Be Determined | May require EID 800 filter adjustment |  | Data onboarding req  Todd |
| EXE-35 | Execution | PowerShell | PowerShell Invoke-RestMethod cmdlet | Not Detected | Activity Logged To Be Determined |  |  | Data onboarding req  IsLogged  Todd |
| EXE-36 | Execution | PowerShell | T1086 - Powershell XML requests | Detected | Critical Severity |  | Splunk |  |
| EXE-37 | Execution | PowerShell | T1086 - Powershell MsXml COM object | Detected | High Severity |  |  |  |
| EXE-38 | Execution | Dynamic Data Exchange | T1173 - Execute Commands | Detected | High Severity |  | Splunk |  |
| EXE-39 | Execution | PowerShell | T1086 - PowerShell Fileless Script Execution | Detected | High Severity |  | Splunk |  |
| EXE-40 | Execution | PowerShell | T1086 - Powershell Invoke-DownloadCradle | Detected | Medium Severity |  |  |  |
| EXE-41 | Execution | Scripting | Macro - Excel 4 | Not Detected | Activity Logged To Be Determined |  |  | Sysmon |
| EXE-42 | Execution | PowerShell | T1086 - Invoke-AppPathBypass | Not Detected | Activity Logged To Be Determined |  |  | Todd |
| EXE-43 | Execution | Scripting | Macro - Obfuscated Cobalt Strike | Not Detected | Activity Logged To Be Determined |  |  | Sysmon |
| EXE-44 | Execution | Scripting | Process Creation Using VBS | Detected | To Be Determined |  | Splunk | Needs work |
| EXE-45 | Execution | PowerShell | Macro - LuckyStrike PowerShell CellEmbed | Blocked | Alert Triggered To Be Determined |  | Windows Defender (Standard) |  |
| EXE-46 | Execution | PowerShell | PowerShell Downgrade | Blocked | Alert Triggered To Be Determined |  |  |  |
| EXE-47 | Execution | Client-side Execution | 10 - DDE - PowerShell | Detected | To Be Determined |  |  |  |
| EXE-48 | Execution | Dynamic Data Exchange | DDE JScript | Detected | High Severity |  | Splunk |  |
| EXE-49 | Execution | JavaScript/JScript | Process Creation Using JScript | Detected | To Be Determined |  |  | Needs work |
| EXE-50 | Execution | Scripting | Macro - Remote Template | Detected | To Be Determined | Once Sysmon is fully deployed that will be logged and with the use case deployed detected | Splunk | Sysmon |
| EXE-51 | Execution | PowerShell | PowerShell New-CimSession | Not Detected | Activity Logged |  |  | Data onboarding req  IsLogged  Todd |
| IMPACT-52 | Impact | Data Encrypted for Impact | Cipher binary execution | Detected | High Severity |  | Splunk | IsLogged |
| IMPACT-53 | Impact | File Deletion | fsutil.exe execution - ransomware | Detected | To Be Determined |  | Splunk | IsLogged |

**Initial Access**

| **Ref #** | **Phase** | **Category** | **Attack Variation** | **Outcome** | **Outcome Details** | **Outcome Notes** | **Detection / Prevention Tools** | **Tags** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ACCESS-1 | Initial Access | Spearphishing Link | Link using Decimal Encoding | Blocked | Alert Triggered To Be Determined |  |  | Testing Completed  NotLogged |
| ACCESS-2 | Initial Access | Spearphishing Link | T1566 - Initial Access - SpearPhishing link leading to file download | Detected | Medium Severity |  | Splunk |  |
| ACCESS-3 | Initial Access | Spearphishing Attachment | Encrypted Attachment sent via Email | Detected | Low Severity |  | Splunk | IsLogged |
| ACCESS-4 | Initial Access | Malicious Link | Phishing Azure Creds via email - malicious link | Blocked | Alert Triggered To Be Determined |  |  | IsLogged |
| ACCESS-5 | Initial Access | Password Spraying | Password Spray against ADFS | Detected | High Severity |  | Splunk |  |
| ACCESS-6 | Initial Access | Spearphishing Attachment | T1193 - Download Phishing Attachment - VBScript | Detected | To Be Determined |  |  | IsLogged  Sysmon |
| ACCESS-7 | Initial Access | Password Spraying | Password Brute Force on ADFS | Detected | Low Severity | ADFS has preventions in place but we still detect this activity | Splunk |  |
| ACCESS-8 | Initial Access | Spearphishing Link | Spoof Sender Address | Detected | To Be Determined |  | Splunk | IsLogged |
| ACCESS-9 | Initial Access | Spearphishing Link | Macro - Remote Template | Detected | To Be Determined |  | Splunk | Sysmon |
| ACCESS-10 | Initial Access | Spearphishing Link | Password-protected Office Document | Detected | To Be Determined | May be picked up by the IronPort use case | Splunk | NotLogged |
| ACCESS-11 | Initial Access | Spearphishing Link | Link to Popular Sharing Service (Drive, Dropbox, etc) | Not Detected | Activity Logged |  |  | IsLogged |
| ACCESS-12 | Initial Access | Trusted Relationship | Send email directly to Office 365 Tenant SMTP | Not Detected | Activity Logged |  |  | IsLogged |

**Linux Threats**

| **Ref #** | **Phase** | **Category** | **Attack Variation** | **Outcome** | **Outcome Details** | **Outcome Notes** | **Detection / Prevention Tools** | **Tags** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| CRED-ACC-1 | Credential Access | Credentials In Files | Reading Bash History & Credentials in Files | Not Detected | Activity Logged To Be Determined |  |  | Vadym |
| PRIV-ESC-2 | Privilege Escalation | Sudo and Sudo Caching | Viewing or Modification of Sudoers file | Not Detected | Activity Logged To Be Determined |  |  | Vadym |
| EXE-3 | Execution | Lateral Tool Transfer | Remote File Copy | Not Detected | Activity Logged To Be Determined |  |  | Vadym |
| DISC-4 | Discovery | Private Keys | Discovery of SSH private keys | Detected | To Be Determined |  |  | Vadym |
| EVAS-5 | Defense Evasion | Internal Proxy | Port Forwarding and Net Cat use | Detected | Medium Severity |  | Splunk | Vadym |
| PRIV-ESC-6 | Privilege Escalation | Boot or Logon Autostart Execution | LNX-T1547 kernel modules | Detected | To Be Determined |  | Splunk |  |
| DISC-7 | Discovery | Network Sniffing | LNX-T1040 Network Sniffing Using Promiscuous Mode | Detected | To Be Determined |  | Splunk |  |
| RECON-8 | Reconnaissance | System Information Discovery | LNX-0016 - Reading SSH keys | Detected | Medium Severity |  |  |  |
| EVAS-9 | Defense Evasion | File and Directory Permissions Modification | LNX-T1222.002 - Permission Mod thru Anomalous File Link | Detected | Low Severity |  | Splunk |  |
| RECON-10 | Reconnaissance | System Information Discovery | LNX-0015 - Reading history files | Detected | To Be Determined |  | Splunk |  |
| PERSIST-11 | Persistence | .bash\_profile and .bashrc | Mddification to Bash RC | Detected | To Be Determined | LNX-0020 - Shell Profile Modification of another user |  | Vadym |
| PERSIST-12 | Persistence | Scheduled Task/Job | Local Job Scheduling - Cron | Detected | To Be Determined |  |  | Needs work  Vadym |
| EVAS-13 | Defense Evasion | Clear Command History | Clear Command History | Not Detected | Activity Logged To Be Determined |  |  | Vadym |
| LAT-MOV-14 | Lateral Movement | Remote Services | SSH for lateral movement | Not Detected | Activity Logged To Be Determined |  |  | Vadym |
| EVAS-15 | Defense Evasion | Timestomp | Timestomping | Not Detected | Activity Logged To Be Determined |  |  | Vadym |
| EVAS-16 | Defense Evasion | Masquerading | Masquarding | Not Detected | Activity Logged To Be Determined |  |  | Vadym |
| PRIV-ESC-17 | Privilege Escalation | Sudo and Sudo Caching | Use of SUDO | Detected | Medium Severity |  |  | Vadym |
| EVAS-18 | Defense Evasion | Process Injection | LNX-T1055 Linux process injection with ptrace | Detected | Medium Severity | LNX-T1055 Process Injection with ptrace | Splunk | Vadym |
| EVAS-19 | Defense Evasion | Hidden Files and Directories | Create Hidden Directory | Not Detected | Activity Logged To Be Determined |  |  | Vadym |
| EVAS-20 | Defense Evasion | Hidden Files and Directories | Create Hidden File | Not Detected | Activity Logged To Be Determined |  |  | Vadym |

**Credential Access**

| **Ref #** | **Phase** | **Category** | **Attack Variation** | **Outcome** | **Outcome Details** | **Outcome Notes** | **Detection / Prevention Tools** | **Tags** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| CRED-ACC-1 | Credential Access | Credential Dumping | T1003 - Powershell Mimikatz | Detected | Critical Severity |  | Splunk |  |
| CRED-ACC-2 | Credential Access | PowerShell | PowerShell to grab CredMgr pws | Not Detected | Activity Logged To Be Determined |  |  | IsLogged |
| CRED-ACC-3 | Credential Access | OS Credential Dumping | New LSASS Dump technique | Not Detected | No Activity Logged |  |  |  |
| CRED-ACC-4 | Credential Access | OS Credential Dumping | Golden SAML - ADFS Dump | Detected | To Be Determined |  | Splunk | Data onboarding req  Testing Completed |
| CRED-ACC-5 | Credential Access | Credentials from Web Browsers | Obtain cookies from Web Browsers | Not Detected | Activity Logged To Be Determined |  |  | Todd  Data Source is unknown |
| CRED-ACC-6 | Credential Access | Credentials from Web Browsers | Dump creds from Browser memory | Not Detected | Activity Logged To Be Determined |  |  | Sysmon |
| CRED-ACC-7 | Credential Access | Credential Dumping | T1003 - Offline Credential Theft With Mimikatz | Detected | Critical Severity |  | Splunk |  |
| CRED-ACC-8 | Credential Access | Credential Dumping | T1003 - Dump LSASS.exe Memory using Windows Task Manager | Detected | To Be Determined |  |  | Sysmon |
| CRED-ACC-9 | Credential Access | Credentials in Files | T1081 - Browser and System credentials | Not Detected | Activity Logged |  |  | Todd |
| CRED-ACC-10 | Credential Access | Credential Dumping | Extract Logonpasswords via Dumpert | Detected | To Be Determined | Based on data from Samir's Att&ck EVTX this would be caught by our current detection | Splunk | Testing Completed |
| CRED-ACC-11 | Credential Access | Kerberoasting | Kerberoasting - RC4 | Detected | Critical Severity |  | Splunk |  |
| CRED-ACC-12 | Credential Access | Credentials in Files | T1081 - Extracting credentials from files | Not Detected | Activity Logged |  |  |  |
| CRED-ACC-13 | Credential Access | Brute Force | T1110 - Brute Force Credentials | Detected | To Be Determined |  | Splunk |  |
| CRED-ACC-14 | Credential Access | Credentials in Registry | T1214 - Enumeration for Credentials in Registry | Not Detected | Activity Logged |  |  |  |
| CRED-ACC-15 | Credential Access | Credential Dumping | T1003 - Dump LSASS.exe Memory using ProcDump | Detected | Critical Severity |  | Splunk |  |
| CRED-ACC-16 | Credential Access | Credential Dumping | T1003 - Dump LSASS.exe Memory using ProcDump w/ -r option | Detected | To Be Determined |  |  | Sysmon |
| CRED-ACC-17 | Credential Access | Credential Dumping | T1003 - Registry dump of SAM, creds, and secrets | Not Detected | Activity Logged |  |  | IsLogged |
| CRED-ACC-18 | Credential Access | Credential Dumping | T1003 - Dump Active Directory Database with NTDSUtil | Detected | To Be Determined |  |  | IsLogged |
| CRED-ACC-19 | Credential Access | Network Sniffing | T1040 - Packet Capture PowerShell | Not Detected | Activity Logged |  |  |  |
| CRED-ACC-20 | Credential Access | Brute Force | Active Directory Password Spray | Not Detected | Activity Logged |  | Splunk | IsLogged |
| CRED-ACC-21 | Credential Access | Brute Force | Active Directory Password Spray - Kerberos | Not Detected | Activity Logged |  |  | IsLogged |
| CRED-ACC-22 | Credential Access | Credential Dumping | Extract Logonpasswords via Mimikatz Binary | Detected | Critical Severity |  | Splunk |  |
| CRED-ACC-23 | Credential Access | Credential Dumping | Impacket DCSync | Detected | High Severity |  | Splunk | Sysmon |
| CRED-ACC-24 | Credential Access | Credential Dumping | Extract Password Hashes via VSS | Detected | To Be Determined |  |  | IsLogged |
| CRED-ACC-25 | Credential Access | Kerberoasting | Kerberoasting | Detected | Critical Severity |  | Splunk |  |
| CRED-ACC-26 | Credential Access | Brute Force | Database Login Brute Force - 1 | Not Detected | Activity Logged To Be Determined |  |  |  |
| CRED-ACC-27 | Credential Access | Credential Dumping | Extract Logonpasswords via SafetyKatz | Detected | Critical Severity |  | Splunk |  |
| CRED-ACC-28 | Credential Access | Credential Dumping | Extract SAM Hashes via Beacon Hashdump | Not Detected | Activity Logged To Be Determined |  |  | Testing Completed |
| CRED-ACC-29 | Credential Access | OS Credential Dumping | Dump lsass with rundll32 & comsvcs.dll | Detected | To Be Determined |  | Splunk | IsLogged |
| CRED-ACC-30 | Credential Access | OS Credential Dumping | ntdsaudit.exe to dump DC hashes | Not Detected | Activity Logged |  |  | IsLogged |
| CRED-ACC-31 | Credential Access | OS Credential Dumping | esentutl.exe to backup ntds.dit | Detected | To Be Determined |  |  | IsLogged |

**SWIFT**

| **Ref #** | **Phase** | **Category** | **Attack Variation** | **Outcome** | **Outcome Details** | **Outcome Notes** | **Detection / Prevention Tools** | **Tags** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ACCESS-1 | Initial Access | Valid Accounts | SWIFT Privilegde Account Used | Detected | To Be Determined |  |  |  |
| LAT-MOV-2 | Lateral Movement | Remote Access Software | SWIFT - New workstation connecting to the VPN | Not Detected | Activity Logged To Be Determined |  |  |  |
| ACCESS-3 | Initial Access | Brute Force | SWIFT Excessive Failed \_A Login Attempts | Detected | To Be Determined |  |  |  |
| ACCESS-4 | Initial Access | Valid Accounts | SWIFT Priv Acc Password Change Time Exceeded | Detected | To Be Determined |  |  |  |
| ACCESS-5 | Initial Access | Valid Accounts | SWIFT - Attempt to use a disabled account | Detected | To Be Determined |  |  |  |
| ACCESS-6 | Initial Access | Valid Accounts | SWIFT Monitored Breakglass Login | Detected | To Be Determined |  |  |  |
| CRED-ACC-7 | Credential Access | Brute Force | SWIFT - (SAA) or (SAG) Swift Server Login Failure | Detected | To Be Determined |  |  |  |
| ACCESS-8 | Initial Access | Valid Accounts | SWIFT Privileged Account checked out of CyberArk | Detected | To Be Determined |  |  |  |
| PRIV-ESC-9 | Privilege Escalation | Domain Groups | SWIFT - User added to privileged group | Detected | To Be Determined |  |  |  |
| CRED-ACC-10 | Credential Access | Brute Force | SWIFT - Brute force against VMware server | Detected | To Be Determined |  |  |  |
| EXE-11 | Execution | Malicious File | SWIFT FEP Detections | Detected | To Be Determined |  |  |  |
| CRED-ACC-12 | Credential Access | Brute Force | SWIFT - Windows wrks or Server brute force | Detected | To Be Determined |  |  |  |

**Azure AD**

| **Ref #** | **Phase** | **Category** | **Attack Variation** | **Outcome** | **Outcome Details** | **Outcome Notes** | **Detection / Prevention Tools** | **Tags** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| PRIV-ESC-1 | Privilege Escalation | Valid Accounts | Rare application consent | Not Detected | Activity Logged To Be Determined |  |  |  |
| ACCESS-2 | Initial Access | Valid Accounts | Attempts to sign in to disabled accounts | Not Detected | Activity Logged To Be Determined |  |  |  |
| ACCESS-3 | Initial Access | Valid Accounts | Successful logon from IP and failure from a different IP | Not Detected | Activity Logged To Be Determined |  |  |  |
| LAT-MOV-4 | Lateral Movement | Valid Accounts | Attempt to bypass conditional access rule in Azure AD | Not Detected | Activity Logged To Be Determined |  |  | High Priority |
| LAT-MOV-5 | Lateral Movement | Valid Accounts | Suspicious application consent similar to PwnAuth | Not Detected | Activity Logged To Be Determined |  |  | High Priority |
| ACCESS-6 | Initial Access | Valid Accounts | Sign-ins from IPs that attempt sign-ins to disabled accounts | Not Detected | Activity Logged To Be Determined |  |  |  |
| IMPACT-7 | Impact | Valid Accounts | Creation of expensive computes in Azure | Not Detected | Activity Logged To Be Determined |  |  |  |
| PRIV-ESC-8 | Privilege Escalation | Cloud Groups | Suspicious granting of permissions to an account | Not Detected | Activity Logged To Be Determined |  |  |  |
| LAT-MOV-9 | Lateral Movement | Valid Accounts | Mail.Read Permissions Granted to Application | Not Detected | Activity Logged To Be Determined |  |  | High Priority |
| LAT-MOV-10 | Lateral Movement | Valid Accounts | Azure Active Directory PowerShell accessing non-AAD resources | Not Detected | Activity Logged To Be Determined |  |  | High Priority |
| LAT-MOV-11 | Lateral Movement | Valid Accounts | Interactive STS refresh token modifications | Not Detected | Activity Logged To Be Determined |  |  | High Priority |
| LAT-MOV-12 | Lateral Movement | Valid Accounts | Legacy Authentication to Azure AD | Not Detected | Activity Logged To Be Determined |  |  | High Priority |
| EVAS-13 | Defense Evasion | Valid Accounts | Suspicious number of resource creation or deployment activities | Not Detected | Activity Logged To Be Determined |  |  |  |
| LAT-MOV-14 | Lateral Movement | Valid Accounts | Modified domain federation trust settings | Not Detected | Activity Logged To Be Determined |  |  | High Priority |
| CRED-ACC-15 | Credential Access | Brute Force | Brute Force Attack against GitHub Account | Not Detected | Activity Logged To Be Determined |  |  |  |
| ACCESS-16 | Initial Access | Valid Accounts | New access credential added to Application or Service Principal | Not Detected | Activity Logged To Be Determined |  |  |  |
| PRIV-ESC-17 | Privilege Escalation | Valid Accounts | Rare subscription-level operations in Azure | Not Detected | Activity Logged To Be Determined |  |  |  |
| EVAS-18 | Defense Evasion | Valid Accounts | Suspicious Resource deployment | Not Detected | Activity Logged To Be Determined |  |  |  |
| ACCESS-19 | Initial Access | Brute Force | Brute force attack against Azure Portal | Not Detected | Activity Logged To Be Determined |  |  |  |
| LAT-MOV-20 | Lateral Movement | Valid Accounts | Suspicious application consent for offline access | Not Detected | Activity Logged To Be Determined |  |  | High Priority |
| ACCESS-21 | Initial Access | Valid Accounts | Distributed Password cracking attempts in AzureAD | Not Detected | Activity Logged To Be Determined |  |  |  |
| ACCESS-22 | Initial Access | Valid Accounts | Successful logon from IP and failure from a different IP | Not Detected | Activity Logged To Be Determined |  |  |  |
| PRIV-ESC-23 | Privilege Escalation | Cloud Groups | User added to Azure Active Directory Privileged Groups | Not Detected | Activity Logged To Be Determined |  |  |  |
| ACCESS-24 | Initial Access | Valid Accounts | Failed login attempts to Azure Portal | Not Detected | Activity Logged To Be Determined |  |  |  |
| ACCESS-25 | Initial Access | Valid Accounts | Anomalous sign-in location by user account and authenticating application | Not Detected | Activity Logged To Be Determined |  |  |  |
| ACCESS-26 | Initial Access | Valid Accounts | Explicit MFA Deny | Not Detected | Activity Logged To Be Determined |  |  |  |
| EXFIL-27 | Exfiltration | Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol | Multiple users email forwarded to same destination | Not Detected | Activity Logged To Be Determined |  |  | High Priority |
| ACCESS-28 | Initial Access | Password Spraying | Password spray attack against Azure AD application | Not Detected | Activity Logged To Be Determined |  |  |  |
| LAT-MOV-29 | Lateral Movement | Valid Accounts | Suspicious application consent similar to O365 Attack Toolkit | Not Detected | Activity Logged To Be Determined |  |  | High Priority |
| EXFIL-30 | Exfiltration | Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol | Mail redirect via ExO transport rule | Not Detected | Activity Logged To Be Determined |  |  | High Priority |
| ACCESS-31 | Initial Access | Valid Accounts | First access credential added to Application or Service Principal where no credential was present | Not Detected | Activity Logged To Be Determined |  |  |  |

**Other Threats or Intel**

| **Ref #** | **Phase** | **Category** | **Attack Variation** | **Outcome** | **Outcome Details** | **Outcome Notes** | **Detection / Prevention Tools** | **Tags** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| EXE-1 | Execution | Masquerading | Parent->Child relationship abnormalities | Not Detected | Activity Logged To Be Determined |  |  |  |
| PERSIST-2 | Persistence | Valid Accounts | Review of trusted system on auth and access | Not Detected | Activity Logged To Be Determined |  |  |  |

**Discovery**

| **Ref #** | **Phase** | **Category** | **Attack Variation** | **Outcome** | **Outcome Details** | **Outcome Notes** | **Detection / Prevention Tools** | **Tags** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| DISC-1 | Discovery | System Information Discovery | GPO & password discovery via SYSVOL share | Not Detected | No Activity Logged |  |  | Data onboarding req |
| DISC-2 | Discovery | Network Service Scanning | T1046 - Discovery - Scanning of web servers on 443 | Detected | High Severity |  | Splunk |  |
| DISC-3 | Discovery | Account Discovery | T1087 - Discovery - Rare process interacting with Directory Services | Detected | To Be Determined |  | Splunk |  |
| DISC-4 | Discovery | Network Service Scanning | T1046 - Discovery - Suspicious SMTP connection from workstation | Detected | Medium Severity |  | Splunk |  |
| DISC-5 | Discovery | Security Software Discovery | psloglist.exe - export etvx logs | Detected | To Be Determined |  | Splunk | IsLogged |
| DISC-6 | Discovery | System Information Discovery | gpresult.exe with flags | Not Detected | Activity Logged |  |  | IsLogged |
| DISC-7 | Discovery | System Information Discovery | Invoke-WMIObject discovery | Not Detected | Activity Logged To Be Determined | May need to modify EID 800 logging |  | Data onboarding req  IsLogged  Todd |
| DISC-8 | Discovery | System Information Discovery | Discovery using ADSI | Not Detected | Activity Logged To Be Determined |  |  | Todd |
| DISC-9 | Discovery | Security Software Discovery | T1063 - Security Software Discovery - powershell | Not Detected | Activity Logged To Be Determined |  |  | Data onboarding req  IsLogged |
| DISC-10 | Discovery | Security Software Discovery | T1063 - Security Software Discovery - Sysmon Service | Detected | To Be Determined |  |  | IsLogged |
| DISC-11 | Discovery | System Network Connections Discovery | T1049 - System Network Connections Discovery | Detected | Medium Severity |  | Splunk | IsLogged |
| DISC-12 | Discovery | System Service Discovery | T1007 - System Service Discovery | Detected | Medium Severity |  | Splunk | IsLogged |
| DISC-13 | Discovery | Remote System Discovery | T1018 - Remote System Discovery - net | Detected | To Be Determined |  | Splunk | IsLogged |
| DISC-14 | Discovery | Query Registry | T1012 - Query Registry | Not Detected | Activity Logged |  |  | IsLogged |
| DISC-15 | Discovery | Account Discovery | T1087 - Enumerate logged on users via PowerShell | Not Detected | Activity Logged To Be Determined |  |  | IsLogged |
| DISC-16 | Discovery | File and Directory Discovery | T1083 - File and Directory Discovery | Not Detected | Activity Logged To Be Determined |  |  | IsLogged |
| DISC-17 | Discovery | Account Discovery | T1087 - Enumerate logged on users | Not Detected | Activity Logged |  |  | IsLogged |
| DISC-18 | Discovery | Account Discovery | T1087 - Enumerate all accounts via PowerShell | Not Detected | Activity Logged To Be Determined |  |  | IsLogged |
| DISC-19 | Discovery | Account Discovery | T1087 - Enumerate all accounts via WMIC | Detected | To Be Determined |  |  | IsLogged |
| DISC-20 | Discovery | Application Window Discovery | T1010 - List Process Main Windows - C# .NET | Not Detected | Activity Logged |  |  | IsLogged |
| DISC-21 | Discovery | Network Share Discovery | T1135 - Network Share Discovery PowerShell | Detected | High Severity |  | Splunk |  |
| DISC-22 | Discovery | Remote System Discovery | T1018 - Remote System Discovery | Detected | To Be Determined |  | Splunk |  |
| DISC-23 | Discovery | System Service Discovery | T1007 - System Service Discovery - net.exe | Detected | Medium Severity |  | Splunk | IsLogged |
| DISC-24 | Discovery | Network Share Discovery | T1135 - Network Share Discovery command prompt | Detected | Medium Severity |  | Splunk | IsLogged |
| DISC-25 | Discovery | Security Software Discovery | T1063 - Security Software Discovery | Not Detected | Activity Logged To Be Determined |  |  | IsLogged |
| DISC-26 | Discovery | Permission Groups Discovery | T1069 - Permission Groups Discovery PowerShell | Not Detected | Activity Logged To Be Determined |  |  | Data onboarding req  IsLogged  Todd |
| DISC-27 | Discovery | Account Discovery | T1087 - Enumerate via cmdkey.exe | Not Detected | Activity Logged |  |  | IsLogged |
| DISC-28 | Discovery | System Owner/User Discovery | T1033 - System Owner/User Discovery | Detected | To Be Determined |  |  | IsLogged |
| DISC-29 | Discovery | Remote System Discovery | BloodHound | Detected | To Be Determined |  |  | Needs work |
| DISC-30 | Discovery | Account Discovery | BloodHound Session Enumeration (No-DC) | Detected | To Be Determined |  | Splunk |  |
| DISC-31 | Discovery | Account Discovery | BloodHound Session Enumeration | Detected | High Severity |  | Splunk |  |
| DISC-32 | Discovery | Network Service Scanning | Internal Port Scan for SSH | Detected | Medium Severity |  | Splunk | Testing Completed  Sysmon |
| DISC-33 | Discovery | Network Service Scanning | Internal Port Scan for RDP | Detected | To Be Determined |  | Splunk |  |
| DISC-34 | Discovery | Permission Groups Discovery | WMIC for group discovery 1 | Detected | To Be Determined |  | Splunk | IsLogged |
| DISC-35 | Discovery | Permission Groups Discovery | WMIC for group discovery 2 | Detected | To Be Determined |  | Splunk | IsLogged |
| DISC-36 | Discovery | Domain Trust Discovery | Nltest - Domain discovery | Detected | Low Severity |  | Splunk | IsLogged |
| DISC-37 | Discovery | Remote System Discovery | Netdom discovery | Detected | To Be Determined |  | Splunk | IsLogged |
| DISC-38 | Discovery | Account Discovery | SPN discovery with setspn | Not Detected | Activity Logged |  |  | IsLogged |
| DISC-39 | Discovery | System Information Discovery | Kerberos ticket discovery | Not Detected | Activity Logged |  |  | IsLogged |
| DISC-40 | Discovery | Security Software Discovery | AppLocker Policy Discovey | Not Detected | Activity Logged To Be Determined |  |  | Testing Completed  Sysmon  High Priority |

**Defense Evasion**

| **Ref #** | **Phase** | **Category** | **Attack Variation** | **Outcome** | **Outcome Details** | **Outcome Notes** | **Detection / Prevention Tools** | **Tags** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| EVAS-1 | Defense Evasion | Trusted Developer Utilities | T1127 - MSBuild Bypass Using Inline Tasks | Detected | Medium Severity |  | Splunk |  |
| EVAS-2 | Defense Evasion | Command and Scripting Interpreter | T1059 - Defense Evasion - Explorer executing script files | Detected | High Severity |  | Splunk |  |
| EVAS-3 | Defense Evasion | User Execution | T1204 - Defense Evasion - Archive image file written to disk | Detected | High Severity |  | Splunk |  |
| EVAS-4 | Defense Evasion | Masquerading | PPID spoofing using Cobalt Strike | Detected | To Be Determined |  |  | Testing Completed  Sysmon |
| EVAS-5 | Defense Evasion | Impair Defenses | T1562 - Defense Evasion - Impair or Modify Windows Defender | Detected | Critical Severity |  | Splunk |  |
| EVAS-6 | Defense Evasion | Disable Windows Event Logging | Disable Sysmon with Shhmon | Detected | To Be Determined |  |  | Testing Completed  Sysmon |
| EVAS-7 | Defense Evasion | Security Software Discovery | PowerShell cmdlets to view or disable Defender settings | Detected | High Severity |  |  | Data onboarding req  Testing Completed |
| EVAS-8 | Defense Evasion | Impair Defenses | T1562 - Defense Evasion - Impair or Modify Windows Defender via WMI | Detected | High Severity |  | Splunk |  |
| EVAS-9 | Defense Evasion | Obfuscated Files or Information | CMD cmdline obfuscation | Detected | To Be Determined |  | Splunk | IsLogged |
| EVAS-10 | Defense Evasion | Hide Artifacts | T1564 - Defense Evasion - Alternate Data Stream execution | Detected | High Severity |  | Splunk |  |
| EVAS-11 | Defense Evasion | Parent PID Spoofing | PPID Spoofing variant | Detected | Medium Severity |  |  | Todd |
| EVAS-12 | Defense Evasion | Process Injection | T1055 - Defense Evasion - Create Remote Thread injection | Detected | High Severity |  | Splunk |  |
| EVAS-13 | Defense Evasion | Impair Defenses | T1562 - Defense Evasion - Unauthorized Sysmon configuration change | Detected | Critical Severity |  | Splunk |  |
| EVAS-14 | Defense Evasion | Signed Binary Proxy Execution | T1218 - Defense Evasion - Rare msiexec child process | Detected | Critical Severity |  | Splunk |  |
| EVAS-15 | Defense Evasion | Obfuscated Files or Information | T1027 - Defense Evasion - Suspicious use of Relative Path | Detected | High Severity |  | Splunk |  |
| EVAS-16 | Defense Evasion | Signed Binary Proxy Execution | T1218 - Defense Evasion - Rare use of Control\_Rundll with Rundll32 | Detected | High Severity |  |  |  |
| EVAS-17 | Defense Evasion | Hijack Execution Flow | T1574 - Defense Evasion - DLL search order hijacking | Detected | High Severity |  |  |  |
| EVAS-18 | Defense Evasion | Disable Windows Event Logging | Disable ETW logs | Detected | To Be Determined |  |  | IsLogged  Sysmon |
| EVAS-19 | Defense Evasion | Hidden Files and Directories | T1158 - Create Windows System File with Attrib | Not Detected | Activity Logged |  |  | IsLogged |
| EVAS-20 | Defense Evasion | Process Injection | T1055 - Process Injection via mavinject.exe | Blocked | Alert Triggered To Be Determined |  | AppLocker | IsLogged |
| EVAS-21 | Defense Evasion | Disable Windows Event Logging | Disable Windows Security Logs - Suspend EventLog Service | Not Detected | Activity Logged To Be Determined |  |  | Sysmon  Data Source is unknown |
| EVAS-22 | Defense Evasion | Indirect Command Execution | T1202 - Indirect Command Execution - pcalua.exe | Detected | Medium Severity |  | Splunk |  |
| EVAS-23 | Defense Evasion | Deobfuscate/Decode Files or Information | T1140 - Certutil Rename and Decode | Not Detected | Activity Logged |  |  | Needs work  IsLogged |
| EVAS-24 | Defense Evasion | Disabling Security Tools | T1089 - Unload Sysmon Filter Driver | Detected | To Be Determined |  |  | IsLogged |
| EVAS-25 | Defense Evasion | File Permissions Modification | T1222 - icacls - Grant permission to specified user or group recursively | Not Detected | Activity Logged |  |  | IsLogged |
| EVAS-26 | Defense Evasion | File Permissions Modification | T1222 - Take ownership recursively using takeown utility | Not Detected | Activity Logged |  |  | IsLogged |
| EVAS-27 | Defense Evasion | File Permissions Modification | T1222 - cacls - Grant permission to specified user or group | Not Detected | Activity Logged |  |  | IsLogged |
| EVAS-28 | Defense Evasion | Process Injection | Process Injection for userland processes | Not Detected | Activity Logged To Be Determined |  |  | Sysmon  High Priority  Todd |
| EVAS-29 | Defense Evasion | Regsvr32 | T1117 - Regsvr32 local COM scriptlet execution | Detected | To Be Determined |  |  | Needs work  IsLogged  Sysmon |
| EVAS-30 | Defense Evasion | Process Injection | Process Injection into Explorer | Detected | To Be Determined | Only detected once Sysmon is rolled out Bank wide and all Sysmon use cases are deployed in Splunk. | Splunk | Sysmon |
| EVAS-31 | Defense Evasion | Regsvr32 | T1117 - Regsvr32 local DLL execution | Detected | To Be Determined |  |  | IsLogged |
| EVAS-32 | Defense Evasion | CMSTP | T1191 - CMSTP Executing UAC Bypass | Detected | Medium Severity |  | Splunk |  |
| EVAS-33 | Defense Evasion | Compiled HTML File | T1223 - Compiled HTML Help Remote Payload | Detected | Medium Severity |  | Splunk |  |
| EVAS-34 | Defense Evasion | Signed Binary Proxy Execution | T1218 - SyncAppvPublishingServer - Execute arbitrary PowerShell code | Detected | Medium Severity |  | Splunk |  |
| EVAS-35 | Defense Evasion | Disable Windows Event Logging | Disable Windows Security Logs - Invoke-Phant0m | Detected | To Be Determined |  | Splunk | Testing Completed  Sysmon |
| EVAS-36 | Defense Evasion | Disable Windows Event Logging | Disable Windows Security Logs - Invoke-GhostLog | Detected | To Be Determined |  |  | Testing Completed  Sysmon |
| EVAS-37 | Defense Evasion | Mshta | T1170 - Mshta executes JavaScript Scheme Fetch Remote Payload With GetObject | Detected | To Be Determined |  | Splunk | IsLogged |
| EVAS-38 | Defense Evasion | Hidden Files and Directories | T1158 - Create Windows Hidden File with Attrib | Not Detected | Activity Logged |  |  | IsLogged |
| EVAS-39 | Defense Evasion | Masquerading | T1036 - Masquerading as Windows LSASS process | Detected | High Severity |  | Splunk |  |
| EVAS-40 | Defense Evasion | BITS Jobs | T1197 - Persist, Download, & Execute | Detected | High Severity |  | Splunk |  |
| EVAS-41 | Defense Evasion | Modify Registry | T1112 - Modify Registry of Local Machine - cmd | Not Detected | Activity Logged To Be Determined |  |  | Sysmon |
| EVAS-42 | Defense Evasion | Process Injection | T1055 - Process Injection via PowerSploit | Detected | To Be Determined |  |  | Sysmon  Todd |
| EVAS-43 | Defense Evasion | Masquerading | Trusted Binary masquerading | Detected | High Severity |  | Splunk |  |
| EVAS-44 | Defense Evasion | Disable or Modify Tools | Create Windows Defender exclusion or turn off features | Detected | High Severity | Need to ensure we have these defender operational events: Event ID 5001 Event ID 5007 Event ID 5013 |  | Data onboarding req  IsLogged |
| EVAS-45 | Defense Evasion | InstallUtil | T1118 - InstallUtil uninstall method call | Detected | Medium Severity |  | Splunk |  |
| EVAS-46 | Defense Evasion | Disabling Security Tools | T1089 - Disable Windows IIS HTTP Logging | Not Detected | Activity Logged |  |  | IsLogged |
| EVAS-47 | Defense Evasion | Access Token Manipulation | T1134 - Access Token Manipulation | Not Detected | Activity Logged To Be Determined |  |  | Todd |
| EVAS-48 | Defense Evasion | Signed Binary Proxy Execution | LOLBAS for indirect execution | Detected | To Be Determined | Need to review LOLBAS detections based on more complete list of LOLBAS. This also applies to lateral movement use cases |  | Needs work |
| EVAS-49 | Defense Evasion | Rootkit | T1014 - Windows Signed Driver Rootkit Test | Detected | High Severity | Detected using T1068 - Privilege Escalation - Suspicious .sys driver executed |  | Todd |
| EVAS-50 | Defense Evasion | File Permissions Modification | T1222 - Take ownership using takeown utility | Not Detected | Activity Logged |  |  | IsLogged |
| EVAS-51 | Defense Evasion | Disable or Modify Tools | Disable Splunk service | Not Detected | Activity Logged To Be Determined |  |  | Data onboarding req  Data Source is unknown |
| EVAS-52 | Defense Evasion | XSL Script Processing | T1220 - MSXSL Bypass using remote files | Not Detected | Activity Logged |  |  | IsLogged |
| EVAS-53 | Defense Evasion | Disable Windows Event Logging | Disable Windows Security Logs - PowerShell log itself | Not Detected | Activity Logged To Be Determined |  |  | Todd |
| EVAS-54 | Defense Evasion | XSL Script Processing | T1220 - MSXSL Bypass using local files | Not Detected | Activity Logged |  |  | IsLogged |
| EVAS-55 | Defense Evasion | Hidden Files and Directories | T1158 - Create ADS command prompt | Detected | To Be Determined |  |  |  |
| EVAS-56 | Defense Evasion | XSL Script Processing | T1220 - WMIC bypass using local XSL file | Detected | To Be Determined |  | Splunk | Needs work  IsLogged |
| EVAS-57 | Defense Evasion | Indirect Command Execution | T1202 - Indirect Command Execution - forfiles.exe | Detected | Medium Severity |  | Splunk |  |
| EVAS-58 | Defense Evasion | File Permissions Modification | T1222 - attrib - Remove read-only attribute | Not Detected | Activity Logged |  |  | IsLogged |
| EVAS-59 | Defense Evasion | Disable Windows Event Logging | Disable Windows Security Logs - Stop Sysmon Service | Detected | High Severity |  |  | Data onboarding req  Data Source is unknown |
| EVAS-60 | Defense Evasion | Disabling Security Tools | Disable Event Log Service | Not Detected | Activity Logged To Be Determined |  |  | Data onboarding req  Data Source is unknown |
| EVAS-61 | Defense Evasion | Modify Registry | T1112 - Modify Registry of Another User Profile | Not Detected | Activity Logged To Be Determined |  |  | Sysmon |
| EVAS-62 | Defense Evasion | NTFS File Attributes | T1096 - Alternate Data Streams (ADS) | Detected | To Be Determined |  | Splunk | IsLogged  Todd |
| EVAS-63 | Defense Evasion | Rundll32 | T1085 - Rundll32 execute JavaScript Remote Payload With GetObject | Detected | To Be Determined |  | Splunk | IsLogged |
| EVAS-64 | Defense Evasion | Disabling Security Tools | Clear Event Logs | Detected | High Severity |  | Splunk | IsLogged |
| EVAS-65 | Defense Evasion | Disable Windows Event Logging | Disable Windows Security Logs - Stop EventLog Service | Detected | High Severity |  | Splunk | Data onboarding req  Sysmon  Data Source is unknown |
| EVAS-66 | Defense Evasion | CMSTP | T1191 - CMSTP Executing Remote Scriptlet | Detected | Medium Severity |  | Splunk |  |
| EVAS-67 | Defense Evasion | Indicator Blocking | Security Tool Network Route Blacklist | Detected | To Be Determined |  |  | IsLogged |
| EVAS-68 | Defense Evasion | BITS Jobs | T1197 - Download & Execute via PowerShell BITS | Detected | High Severity |  | Splunk |  |
| EVAS-69 | Defense Evasion | Hidden Files and Directories | T1158 - Create ADS PowerShell | Detected | To Be Determined |  |  | Todd |
| EVAS-70 | Defense Evasion | Deobfuscate/Decode Files or Information | T1140 - Deobfuscate/Decode Files Or Information | Not Detected | Activity Logged |  |  | IsLogged |
| EVAS-71 | Defense Evasion | Compiled HTML File | T1223 - Compiled HTML Help Local Payload | Detected | To Be Determined |  |  | Needs work  IsLogged |
| EVAS-72 | Defense Evasion | BITS Jobs | T1197 - Download & Execute | Detected | High Severity |  | Splunk |  |
| EVAS-73 | Defense Evasion | XSL Script Processing | T1220 - WMIC bypass using remote XSL file | Detected | Medium Severity |  | Splunk |  |
| EVAS-74 | Defense Evasion | File Permissions Modification | T1222 - cacls - Grant permission to specified user or group recursively | Not Detected | Activity Logged |  |  | IsLogged |
| EVAS-75 | Defense Evasion | Signed Binary Proxy Execution | T1218 - mavinject - Inject DLL into running process | Detected | To Be Determined |  |  | IsLogged |
| EVAS-76 | Defense Evasion | Modify Registry | T1112 - Modify Registry of Current User Profile - cmd | Not Detected | Activity Logged To Be Determined |  |  | Sysmon |
| EVAS-77 | Defense Evasion | File Permissions Modification | T1222 - icacls - Grant permission to specified user or group | Not Detected | Activity Logged |  |  | IsLogged |
| EVAS-78 | Defense Evasion | Regsvr32 | T1117 - Regsvr32 remote COM scriptlet execution | Detected | Medium Severity |  | Splunk | Sysmon |
| EVAS-79 | Defense Evasion | Obfuscated Files or Information | Obfuscated Commands - PowerShell | Not Detected | Activity Logged To Be Determined |  |  |  |
| EVAS-80 | Defense Evasion | Obfuscated Files or Information | Obfuscated Commands - CMD | Not Detected | Activity Logged To Be Determined |  |  |  |
| EVAS-81 | Defense Evasion | Masquerading | T1036 - Defense Evasion - Renamed system binary executed | Detected | To Be Determined | Detection using sysmon EventID1 | Splunk |  |

**Lateral Movement**

| **Ref #** | **Phase** | **Category** | **Attack Variation** | **Outcome** | **Outcome Details** | **Outcome Notes** | **Detection / Prevention Tools** | **Tags** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| LAT-MOV-1 | Lateral Movement | Remote Desktop Protocol | RDP Mirroring | Not Detected | Activity Logged |  |  | IsLogged |
| LAT-MOV-2 | Lateral Movement | Exploitation of Remote Services | T1210 - Lateral Movement - Impacket or PetitPotam usage | Detected | Critical Severity |  | Splunk |  |
| LAT-MOV-3 | Lateral Movement | Steal or Forge Kerberos Tickets | Mimikatz OverPtH | Detected | High Severity |  | Splunk |  |
| LAT-MOV-4 | Lateral Movement | Remote Desktop Protocol | T1076 - RDP highjacking | Not Detected | Activity Logged |  |  | IsLogged |
| LAT-MOV-5 | Lateral Movement | Windows Management Instrumentation | WMI remote exec of MSI | Detected | To Be Determined |  |  | Needs work  IsLogged |
| LAT-MOV-6 | Lateral Movement | Windows Service | Remote Service Creation using sc.exe | Detected | To Be Determined |  | Splunk | IsLogged |
| LAT-MOV-7 | Lateral Movement | Remote Desktop Protocol | SharpRDP | Detected | To Be Determined |  |  | Sysmon |
| LAT-MOV-8 | Lateral Movement | Windows Remote Management | WinRS binary | Detected | High Severity |  | Splunk |  |
| LAT-MOV-9 | Lateral Movement | Steal or Forge Kerberos Tickets | Rubeus OverPtH | Detected | High Severity |  | Splunk |  |
| LAT-MOV-10 | Lateral Movement | Steal or Forge Kerberos Tickets | Rubeus Monitor function | Not Detected | Activity Logged |  |  | Sysmon |
| LAT-MOV-11 | Lateral Movement | Windows Remote Management | T1028 - Psexec | Detected | Medium Severity | \*\*Whitelisting of the WITOOLS servers is used | Splunk |  |
| LAT-MOV-12 | Lateral Movement | Windows Remote Management | T1028 - Psexec clone - impacket | Detected | High Severity |  |  |  |
| LAT-MOV-13 | Lateral Movement | Pass the Hash | Horizontal Pass-the-Hash | Detected | High Severity |  | Splunk | Needs work |
| LAT-MOV-14 | Lateral Movement | Windows Remote Management | T1028 - PowerShell Lateral Movement | Detected | To Be Determined |  | Splunk | IsLogged |
| LAT-MOV-15 | Lateral Movement | Windows Admin Shares | T1077 - Map Admin Share PowerShell | Not Detected | Activity Logged To Be Determined |  |  | Data onboarding req  IsLogged |
| LAT-MOV-16 | Lateral Movement | Windows Remote Management | T1028 - Enable Windows Remote Management | Not Detected | Activity Logged To Be Determined |  |  | Data onboarding req  IsLogged |
| LAT-MOV-17 | Lateral Movement | Windows Remote Management | T1028 - WMIC Process Call Create | Detected | High Severity |  | Splunk |  |
| LAT-MOV-18 | Lateral Movement | Windows Admin Shares | T1077 - Map admin share | Not Detected | Activity Logged To Be Determined |  |  | IsLogged |
| LAT-MOV-19 | Lateral Movement | Windows Remote Management | T1028 - Invoke-Command | Not Detected | No Activity Logged | Would need to update EID 800 filtering |  | Data onboarding req  Testing Completed  IsLogged |
| LAT-MOV-20 | Lateral Movement | Windows Remote Management | T1028 - Invoke-Command - wsmprovhost.exe | Detected | High Severity |  | Splunk |  |
| LAT-MOV-21 | Lateral Movement | Pass the Hash | T1075 - Mimikatz Kerberos Ticket Attack | Detected | To Be Determined |  | Splunk | Todd |
| LAT-MOV-22 | Lateral Movement | Pass the Hash | T1075 - Mimikatz Pass the Hash | Detected | High Severity |  | Splunk |  |
| LAT-MOV-23 | Lateral Movement | Windows Admin Shares | Lateral Movement via PSExec | Detected | High Severity |  | Splunk |  |
| LAT-MOV-24 | Lateral Movement | Windows Admin Shares | Lateral Movement via SMB Beacon | Not Detected | Activity Logged | Can be detected using EID 5145, see FireEye Github for IOCs |  | IsLogged |
| LAT-MOV-25 | Lateral Movement | Windows Remote Management | Lateral Movement via WinRM | Detected | To Be Determined |  | Splunk | Todd |
| LAT-MOV-26 | Lateral Movement | Distributed Component Object Model | Lateral Movement via WMI | Detected | High Severity |  | Splunk |  |
| LAT-MOV-27 | Lateral Movement | Distributed Component Object Model | Lateral Movement via MMC | Detected | To Be Determined |  | Splunk | Todd |
| LAT-MOV-28 | Lateral Movement | Remote Desktop Protocol | Interactive Logon to a DC | Not Detected | Activity Logged |  |  | IsLogged |
| LAT-MOV-29 | Lateral Movement | Lateral Tool Transfer | Remote File Copy - Wrks to Server | Detected | High Severity |  | Splunk |  |
| LAT-MOV-30 | Lateral Movement | Lateral Tool Transfer | Remote File Copy - Server to Wrks | Detected | High Severity |  | Splunk |  |
| LAT-MOV-31 | Lateral Movement | Windows Service | SCShell tool | Detected | To Be Determined |  |  | Testing Completed  IsLogged |
| LAT-MOV-32 | Lateral Movement | Modify Registry | Remote Registry modification | Not Detected | No Activity Logged |  |  | Sysmon |

**Collection**

| **Ref #** | **Phase** | **Category** | **Attack Variation** | **Outcome** | **Outcome Details** | **Outcome Notes** | **Detection / Prevention Tools** | **Tags** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| COLL-1 | Collection | Data Staged | T1074 - Stage data from Discovery.bat | Not Detected | Activity Logged | This will be detected only because of the use of powershell...execute anyways and look for other detection logic |  |  |
| COLL-2 | Collection | Automated Collection | T1119 - Automated Collection PowerShell | Not Detected | Activity Logged To Be Determined |  |  | Data onboarding req |
| COLL-3 | Collection | Input Capture | T1056 - Input Capture | Not Detected | Activity Logged To Be Determined |  |  |  |
| COLL-4 | Collection | Clipboard Data | T1115 - PowerShell | Not Detected | Activity Logged To Be Determined |  | Splunk |  |
| COLL-5 | Collection | Keylogging | Keylogger PoC | Not Detected | Activity Logged To Be Determined |  |  |  |
| COLL-6 | Collection | Archive Collected Data | Preparing an archive for exfil using 7zip | Detected | To Be Determined |  |  |  |
| COLL-7 | Collection | Automated Collection | T1119 - Automated Collection Command Prompt | Not Detected | Activity Logged To Be Determined |  |  |  |
| COLL-8 | Collection | Clipboard Data | Clipboard data - C# | Not Detected | Activity Logged To Be Determined |  |  | Todd |
| COLL-9 | Collection | Audio Capture | T1123 - SourceRecorder via Windows command prompt | Not Detected | Activity Logged To Be Determined |  |  |  |
| COLL-10 | Collection | Screen Capture | Misuse of PSR.exe | Not Detected | Activity Logged |  |  | IsLogged |
| COLL-11 | Collection | Audio Capture | T1123 - PowerShell Cmdlet via Windows command prompt | Not Detected | Activity Logged To Be Determined |  |  |  |
| COLL-12 | Collection | Clipboard Data | T1115 - Utilize Clipboard to store or execute commands from | Not Detected | Activity Logged To Be Determined |  |  |  |

**Persistence**

| **Ref #** | **Phase** | **Category** | **Attack Variation** | **Outcome** | **Outcome Details** | **Outcome Notes** | **Detection / Prevention Tools** | **Tags** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| PERSIST-1 | Persistence | Registry Run Keys / Startup Folder | T1060 - Startup Folder | Detected | To Be Determined |  |  | High Priority |
| PERSIST-2 | Persistence | External Remote Services | Cisco VPN rogue connection | Not Detected | Activity Logged |  |  | IsLogged |
| PERSIST-3 | Persistence | Component Object Model Hijacking | T1122 - Component Object Model Hijacking | Not Detected | Activity Logged To Be Determined |  |  | Sysmon |
| PERSIST-4 | Persistence | Accessibility Features | Accessibility Features | Detected | To Be Determined |  |  | Sysmon |
| PERSIST-5 | Persistence | Scheduled Task | Scheduled Task modification a la APT29/32 | Detected | High Severity |  | Splunk | High Priority |
| PERSIST-6 | Persistence | Browser Extensions | T1176 - Chrome (Chrome Web Store) | Not Detected | Activity Logged To Be Determined |  |  | Sysmon  Data Source is unknown |
| PERSIST-7 | Persistence | SQL Stored Procedures | Persistence through SQL xp\_cmdshell stored procedure | Detected | High Severity |  | Splunk |  |
| PERSIST-8 | Persistence | Account Manipulation | T1098 - Admin Account Manipulate | Not Detected | No Activity Logged |  |  | NotLogged |
| PERSIST-9 | Persistence | New Service | T1050 - Service Installation | Detected | To Be Determined |  |  | IsLogged |
| PERSIST-10 | Persistence | Winlogon Helper DLL | T1004 - Winlogon Userinit Key Persistence - PowerShell | Detected | To Be Determined |  |  | IsLogged  High Priority |
| PERSIST-11 | Persistence | Scheduled Task | Create schtask using PowerShell | Detected | To Be Determined |  |  | Testing Completed |
| PERSIST-12 | Persistence | Scheduled Task | Create schtask with \XML | Detected | High Severity |  | Splunk | Needs work |
| PERSIST-13 | Persistence | Logon Scripts | T1037 - Logon Scripts | Detected | To Be Determined |  |  | High Priority |
| PERSIST-14 | Persistence | Modify Existing Service | T1031 - Modify Fax service to run PowerShell | Detected | High Severity |  | Splunk |  |
| PERSIST-15 | Persistence | New Service | T1050 - Service Installation PowerShell Installs A Local Service using PowerShell | Detected | To Be Determined |  |  | Testing Completed |
| PERSIST-16 | Persistence | Registry Run Keys / Startup Folder | T1060 - Reg Key RunOnce | Not Detected | Activity Logged To Be Determined |  |  | Sysmon |
| PERSIST-17 | Persistence | Registry Run Keys / Startup Folder | T1060 - Reg Key Run | Not Detected | Activity Logged To Be Determined |  |  |  |
| PERSIST-18 | Persistence | Browser Extensions | T1176 - Firefox | Not Detected | Activity Logged To Be Determined |  |  |  |
| PERSIST-19 | Persistence | Browser Extensions | T1176 - Chrome (Developer Mode) | Not Detected | Activity Logged To Be Determined |  |  |  |
| PERSIST-20 | Persistence | Office Application Startup | T1137 - Persistence - New MS Office Add-in file written | Detected | High Severity |  | Splunk |  |
| PERSIST-21 | Persistence | Create Account | T1136 - Create a new user in a command prompt | Not Detected | Activity Logged |  |  |  |
| PERSIST-22 | Persistence | Registry Run Keys / Startup Folder | T1060 - PowerShell Registry RunOnce | Not Detected | Activity Logged To Be Determined |  |  | Sysmon |
| PERSIST-23 | Persistence | Scheduled Task | Modify a schtask with PowerShell | Not Detected | Activity Logged |  |  | Testing Completed |
| PERSIST-24 | Persistence | Hijack Execution Flow | T1574 - Persistence - Possible DLL Hijacking for application in AppData | Detected | High Severity |  | Splunk |  |
| PERSIST-25 | Persistence | Scheduled Task/Job | T1053 - Persistence - Scheduled Task DLL loaded by untrusted process | Detected | High Severity |  | Splunk |  |
| PERSIST-26 | Persistence | Scheduled Task/Job | T1053 - Persistence - Scheduled Task created to run suspicious binary | Detected | High Severity |  | Splunk |  |
| PERSIST-27 | Persistence | Scheduled Task | Using at.exe to create/execute a task | Detected | To Be Determined |  |  | Testing Completed |
| PERSIST-28 | Persistence | Scheduled Task | Remote Scheduled Task | Detected | High Severity |  | Splunk |  |
| PERSIST-29 | Persistence | LSASS Driver | Mimikatz Mimidrv | Not Detected | Activity Logged To Be Determined |  |  | Sysmon |
| PERSIST-30 | Persistence | Winlogon Helper DLL | T1004 - Winlogon Shell Key Persistence - PowerShell | Not Detected | Activity Logged To Be Determined |  |  | Sysmon |
| PERSIST-31 | Persistence | Scheduled Task/Job | T1053 - Persistence - Scheduled Task created with Impacket AtExec | Detected | Critical Severity |  | Splunk |  |
| PERSIST-32 | Persistence | Scheduled Task | Scheduled Task creation | Detected | To Be Determined | Alerts only on certain binaries being set or \XML files being referenced. | Splunk | Needs work |
| PERSIST-33 | Persistence | Scheduled Task | AtExec scheduled task creation | Detected | To Be Determined |  | Splunk | Testing Completed |
| PERSIST-34 | Persistence | Winlogon Helper DLL | T1004 - Winlogon Notify Key Logon Persistence - PowerShell | Not Detected | Activity Logged To Be Determined |  |  | Sysmon |
| PERSIST-35 | Persistence | Windows Management Instrumentation Event Subscription | WMI Event Subscription | Detected | High Severity |  | Splunk |  |
| PERSIST-36 | Persistence | Web Shell | Webshell - IIS varients | Not Detected | Activity Logged To Be Determined |  |  |  |
| PERSIST-37 | Persistence | Create Account | T1136 - Create a new user in PowerShell | Detected | To Be Determined |  |  | Data onboarding req |
| PERSIST-38 | Persistence | Create Account | New Local Administrator | Detected | To Be Determined |  | Splunk | IsLogged |
| PERSIST-39 | Persistence | Registry Run Keys / Startup Folder | Registry Run Key | Not Detected | Activity Logged To Be Determined |  |  | Sysmon |
| PERSIST-40 | Persistence | Registry Modification | Use of common Run keys to maintain persistence using .BAT file | Not Detected | Activity Logged To Be Determined |  |  | Sysmon |
| PERSIST-41 | Persistence | New Service | New Windows Service | Detected | To Be Determined |  |  |  |
| PERSIST-42 | Persistence | Create Account | Create a Domain Admin | Not Detected | Activity Logged | EventCode=4720 |  |  |
| PERSIST-43 | Persistence | Modify Existing Service | Modify Windows Service | Detected | To Be Determined |  |  |  |

**Exfiltration**

| **Ref #** | **Phase** | **Category** | **Attack Variation** | **Outcome** | **Outcome Details** | **Outcome Notes** | **Detection / Prevention Tools** | **Tags** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| EXFIL-1 | Exfiltration | Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol | Attaching screenshots to email sent externally | Not Detected | Activity Logged To Be Determined |  |  | Sysmon |
| EXFIL-2 | Exfiltration | Exfiltration Over Alternative Protocol | Send to external inbox - Large Attachments | Not Detected | Activity Logged |  |  |  |