| **Initial Access** | T1566 - Phishing | T1566.001 - Spearphishing Attachment | **Critical** | Monitor email attachments for malicious file types and suspicious email patterns | Email Security Logs, SMTP Logs, Attachment Analysis, Threat Intelligence Feeds | title: Suspicious Email Attachments logsource: category: email detection: selection: AttachmentExtension: - '.exe' - '.scr' - '.zip' - '.doc' - '.docm' condition: selection level: critical | | **Initial Access** | T1566 - Phishing | T1566.002 - Spearphishing Link | **Critical** | Monitor for suspicious URLs in emails and user clicks on malicious links | Email Security Logs, Web Proxy Logs, DNS Logs, URL Analysis | title: Suspicious URLs in Email logsource: category: email detection: selection: EmailBody|contains: - 'bit.ly' - 'tinyurl.com' - 'suspicious-domain.com' condition: selection level: critical | | **Initial Access** | T1566 - Phishing | T1566.003 - Spearphishing via Service | **High** | Monitor for phishing attempts through third-party services like social media platforms | Application Logs, API Logs, Social Media Monitoring | title: Phishing via Third-party Services logsource: category: application detection: selection: Service: - 'facebook' - 'twitter' - 'linkedin' MessageContent|contains: 'click here' condition: selection level: high | | **Persistence** | T1547 - Boot or Logon Autostart Execution | T1547.001 - Registry Run Keys / Startup Folder | **High** | Monitor modifications to registry run keys and startup folder additions | Windows Registry Monitoring, Sysmon Event ID 13, File System Monitoring | title: Registry Run Key Modifications logsource: category: registry_set detection: selection: TargetObject|contains: - '\Run\' - '\RunOnce\' - '\RunServices\' condition: selection level: high | | **Persistence** | T1547 - Boot or Logon Autostart Execution | T1547.003 - Time Providers | **Medium** | Monitor changes to time provider configurations | Registry Monitoring, System Configuration Logs | title: Time Provider Modifications logsource: category: registry_set detection: selection: TargetObject|contains: '\TimeProviders\' condition: selection level: medium | | **Persistence** | T1547 - Boot or Logon Autostart Execution | T1547.004 - Winlogon Helper DLL | **High** | Monitor winlogon registry modifications | Registry Monitoring, Sysmon Event ID 13 | title: Winlogon Helper DLL Modification logsource: category: registry_set detection: selection: TargetObject|contains: - '\Winlogon\Notify\' - '\Winlogon\Userinit\' - '\Winlogon\Shell\' condition: selection level: high | | **Persistence** | T1547 - Boot or Logon Autostart Execution | T1547.009 - Shortcut Modification | **Medium** | Monitor for changes to shortcut files (.lnk) in startup locations | File System Monitoring, Sysmon Event ID 11 | title: Startup Shortcut Modifications logsource: category: file_event detection: selection: TargetFilename|endswith: '.lnk' TargetFilename|contains: - '\Startup\' - '\Start Menu\' condition: selection level: medium | | **Privilege Escalation** | T1548 - Abuse Elevation Control Mechanism | T1548.002 - Bypass User Account Control | **High** | Monitor for UAC bypass techniques and unexpected elevation of privileges | Windows Security Logs, UAC Event Logs, Process Monitoring | title: UAC Bypass Attempt logsource: category: process_creation detection: selection: Image|endswith: - '\fodhelper.exe' - '\computerdefaults.exe' IntegrityLevel: 'High' condition: selection level: high | | **Defense Evasion** | T1562 - Impair Defenses | T1562.001 - Disable or Modify Tools | **Critical** | Monitor attempts to disable or modify security tools like Windows Defender | Security Tool Logs, Registry Monitoring, Service Control Logs | title: Security Tool Disabling logsource: category: process_creation detection:

selection: CommandLine|contains: - 'Set-MpPreference -DisableRealtimeMonitoring' - 'sc stop windefend' - 'netsh advfirewall set' condition: selection | level: critical | | **Credential Access** | T1555 - Credentials from Password Stores | T1555.001 - Keychain | **Critical** | Monitor access to credential storage mechanisms | Keychain Access Logs, Process Monitoring, API Call Monitoring | title: Keychain Access Attempt | logsource: category: process_creation | detection: selection: Image|endswith: '/security' CommandLine|contains: - 'dump-keychain' - 'find-generic-password' condition: selection | level: critical | | **Credential Access** | T1555 - Credentials from Password Stores | T1555.003 - Credentials from Web Browsers | **Critical** | Monitor browser credential store access | Browser Logs, Process Monitoring, File Access Logs | title: Browser Credential Theft | logsource: category: file_access | detection: selection: TargetFilename|endswith: - '\Login Data' - '\logins.json' - '\signons.sqlite' condition: selection | level: critical | | **Discovery** | T1082 - System Information Discovery | N/A | **Low** | Monitor for commands that gather system information (systeminfo, whoami, uname) | Command Line Auditing, Process Monitoring, System Logs | title: System Information Discovery | logsource: category: process_creation | detection: selection: Image|endswith: - '\systeminfo.exe' - '\whoami.exe' - '\hostname.exe' condition: selection | level: low | | **Discovery** | T1083 - File and Directory Discovery | N/A | **Low** | Monitor for file enumeration commands (dir, ls, find) | File System Monitoring, Command Line Auditing | title: File and Directory Discovery | logsource: category: process_creation | detection: selection: Image|endswith: - '\dir.exe' - '\tree.exe' CommandLine|contains: - '/s' - '-R' condition: selection | level: low | | **Discovery** | T1135 - Network Share Discovery | N/A | **Medium** | Monitor for network share enumeration (net view, showmount) | Network Monitoring, SMB Logs, Command Line Auditing | title: Network Share Discovery | logsource: category: process_creation | detection: selection: Image|endswith: '\net.exe' CommandLine|contains: - 'view' - 'share' condition: selection | level: medium | | **# MITRE ATT&CK Security Detection Rules Library

This comprehensive table provides detection rules based on the MITRE ATT&CK framework, organized by tactics, techniques, and sub-techniques with corresponding detection logic and required technology logs.

Detection Rules Table

MITRE Category	MITRE Technique	MITRE Sub-technique	Severity	Detection Rule	Technology Logs	Sig
Defense Evasion	T1055 - Process Injection	T1055.001 - Dynamic-link Library Injection	**High**	Monitor DLL/PE file events, specifically creation of these binary files as well as the loading of DLLs into processes. Look for DLLs that are not recognized or not normally loaded into a process.	Sysmon Event ID 7 (Image loaded), Windows Security Event Logs, Process Monitoring, API Call Monitoring (CreateRemoteThread, VirtualAllocEx, WriteProcessMemory)	tit Loa cat `de Ima
Defense Evasion	T1055 - Process Injection	T1055.001 - Dynamic-link Library Injection	**High**	Search for remote thread creations that start at LoadLibraryA or LoadLibraryW. Monitor for processes being viewed that may inject DLLs.	Sysmon Event ID 8 (CreateRemoteThread), Windows Security Logs, EDR/XDR Process Telemetry	tit Cre Loa log cre `de Sta
Defense Evasion	T1055 - Process Injection	T1055.001 - Dynamic-link Library Injection	**High**	Monitor for process memory inconsistencies compared to DLL files on disk by checking memory ranges against a known copy of the legitimate module.	Memory Analysis Tools, Process Memory Dumps, Volatility Framework	tit Inc De cat pro `de Gra '0x
Defense Evasion	T1055 - Process Injection	T1055.001 - Dynamic-link Library Injection	**High**	Detect DLL Injection with Mavinject: Monitor execution of mavinject.exe with	Sysmon Event ID 1 (Process Creation), Windows Security Event ID 4688, Command Line Auditing	tit Inje cat pro `de Ima

MITRE Category	MITRE Technique	MITRE Sub-technique	Severity	Detection Rule	Technology Logs	Sig
				"/INJECTRUNNING" parameter		
Defense Evasion	T1055 - Process Injection	T1055.002 - Portable Executable Injection	**High**	Monitor for processes being viewed that may inject portable executables into processes to evade detection	Sysmon Event ID 8 (CreateRemoteThread), Process Monitoring, EDR/XDR Telemetry	tit Exe log cre `de Tar
Defense Evasion	T1055 - Process Injection	T1055.003 - Thread Execution Hijacking	**High**	Monitor for changes made to processes that may hijack threads of execution to evade detection	Thread Monitoring, Process Hollowing Detection, EDR/XDR Behavioral Analysis	tit Exe log pro `de Gra '0x Cal
Defense Evasion	T1055 - Process Injection	T1055.004 - Asynchronous Procedure Call	**High**	Monitor Windows API calls indicative of APC injection including QueueUserAPC and SetThreadContext	API Call Monitoring, Sysmon Event ID 8, EDR/XDR API Telemetry	tit De cat cre `de Sta
Defense Evasion	T1055 - Process Injection	T1055.005 - Thread Local Storage	**Medium**	Monitor for changes to TLS callback pointers that may be used to redirect processes to malicious code	Memory Analysis, Process Monitoring, TLS Callback Analysis	tit Inje cat pro `de Ima
Defense Evasion	T1055 - Process Injection	T1055.008 - Ptrace System Calls	**Medium**	Monitor ptrace system calls that could indicate process injection on Linux systems	Linux Audit Logs (auditd), System Call Monitoring, strace, ftrace	tit Inje log auc sel

MITRE Category	MITRE Technique	MITRE Sub-technique	Severity	Detection Rule	Technology Logs	Sig
						'SY 'ptr cor lev
Defense Evasion	T1055 - Process Injection	T1055.009 - Proc Memory	**Medium**	Monitor /proc/[pid]/mem access patterns and unusual writes to process memory	Linux Audit Logs, Process File Descriptor Monitoring, inotify	tit Inje log auc sel nar
Defense Evasion	T1055 - Process Injection	T1055.011 - Extra Window Memory Injection	**Medium**	Monitor for process being viewed that may inject code into Extra Window Memory of GUI process on Windows	Windows API Monitoring (GetWindowLong, SetWindowLong), Process Monitoring	tit Me log pro `de Gra '0x
Defense Evasion	T1055 - Process Injection	T1055.012 - Process Hollowing	**Critical**	Monitor for process hollowing by analyzing process memory inconsistencies and unexpected process behavior	Sysmon Event ID 1, Process Creation Monitoring, Memory Analysis, Behavioral Analysis	tit Ho log pro `de Ima
Defense Evasion	T1055 - Process Injection	T1055.013 - Process Doppelgänging	**High**	Monitor for transactional NTFS operations and process creation from transacted files	Windows Security Logs, File System Monitoring, NTFS Transaction Logs	tit Do De cat `de Tar
Defense Evasion	T1055 - Process Injection	T1055.014 - VDSO Hijacking	**Medium**	Monitor for modifications to VDSO memory segments and	Linux Audit Logs, Memory Monitoring, System Call Tracing	tit Lin cat `de

MITRE Category	MITRE Technique	MITRE Sub-technique	Severity	Detection Rule	Technology Logs	Sig
				unexpected system call behavior on Linux		typ sys
Defense Evasion	T1055 - Process Injection	T1055.015 - ListPlanting	**Medium**	Monitor for abuse of list-view controls to inject code into hijacked processes	Windows API Monitoring, Process Behavior Analysis, GUI Component Monitoring	tit Inje cat pro `de Gra '0x
Execution	T1059 - Command and Scripting Interpreter	T1059.001 - PowerShell	**Critical**	Monitor PowerShell execution including encoded commands, suspicious cmdlets, and remote execution	Windows PowerShell Logs (Event ID 4103, 4104), Sysmon Event ID 1, Command Line Auditing	tit Pov log pro `de Ima
Execution	T1059 - Command and Scripting Interpreter	T1059.001 - PowerShell	**Critical**	Detect execution of Base64-encoded PowerShell commands and potentially malicious cmdlets	PowerShell Script Block Logging, Module Logging, Transcription Logging	tit Bas Co log ps_ sel Scr
Execution	T1059 - Command and Scripting Interpreter	T1059.001 - PowerShell	**Critical**	Monitor for PowerShell processes with suspicious parent processes or command line arguments	Sysmon Event ID 1, Windows Security Event ID 4688, EDR/XDR Process Telemetry	tit Spa Sus log pro `de Ima
Execution	T1059 - Command and	T1059.001 - PowerShell	**High**	Detect PowerShell Constrained	PowerShell Event Logs, Security Event Logs, Application Logs	tit Byp cat

MITRE Category	MITRE Technique	MITRE Sub-technique	Severity	Detection Rule	Technology Logs	Sig
	Scripting Interpreter			Language Mode bypasses		`de Scr
Execution	T1059 - Command and Scripting Interpreter	T1059.002 - AppleScript	**Medium**	Monitor AppleScript execution through osascript and AppleScript Editor	macOS System Logs, Process Monitoring, Application Execution Logs	tit Ap log pro `de Ima
Execution	T1059 - Command and Scripting Interpreter	T1059.003 - Windows Command Shell	**High**	Monitor cmd.exe execution with suspicious parameters, obfuscated commands, and chaining techniques	Sysmon Event ID 1, Windows Security Event ID 4688, Command Line Auditing	tit Exe cat pro `de Ima
Execution	T1059 - Command and Scripting Interpreter	T1059.003 - Windows Command Shell	**High**	Detect command line obfuscation using carets, commas, and quotes	Command Line Analysis, Pattern Matching, Behavioral Analytics	tit Ob Tec log pro `de Ima
Execution	T1059 - Command and Scripting Interpreter	T1059.004 - Unix Shell	**High**	Monitor Unix shell execution including bash, sh, zsh, and suspicious shell commands	Linux/Unix Audit Logs (auditd), Shell History, Process Monitoring	tit She log pro `de Ima
Execution	T1059 - Command and Scripting Interpreter	T1059.005 - Visual Basic	**Critical**	Monitor VBA macro execution in Office documents and VBScript execution	Office Application Logs, Windows Script Host Logs, Process Monitoring	tit VB Exe cat pro

MITRE Category	MITRE Technique	MITRE Sub-technique	Severity	Detection Rule	Technology Logs	Sig `de Ima
Execution	T1059 - Command and Scripting Interpreter	T1059.006 - Python	**Medium**	Monitor Python script execution and suspicious Python modules	Process Monitoring, Python Logs, System Call Monitoring	tit Pyt log pro `de Ima
Execution	T1059 - Command and Scripting Interpreter	T1059.007 - JavaScript/JScript	**High**	Monitor JavaScript execution through Windows Script Host, browsers, and Node.js	Windows Script Host Logs, Browser Logs, Process Monitoring	tit Jav log pro `de Ima
Execution	T1059 - Command and Scripting Interpreter	T1059.008 - Network Device CLI	**Critical**	Monitor command line interface access to network devices and configuration changes	Network Device Logs, SNMP Logs, SSH/Telnet Session Logs, Configuration Change Logs	tit Co Ch cat `de Eve 'co Co
Initial Access	T1566 - Phishing	T1566.001 - Spearphishing Attachment	**Critical**	Monitor email attachments for malicious file types and suspicious email patterns	Email Security Logs, SMTP Logs, Attachment Analysis, Threat Intelligence Feeds	
Initial Access	T1566 - Phishing	T1566.002 - Spearphishing Link	**Critical**	Monitor for suspicious URLs in emails and user clicks on malicious links	Email Security Logs, Web Proxy Logs, DNS Logs, URL Analysis	
Initial Access	T1566 - Phishing	T1566.003 - Spearphishing via	**High**	Monitor for phishing attempts	Application Logs, API Logs, Social Media	

MITRE Category	MITRE Technique	MITRE Sub-technique	Severity	Detection Rule	Technology Logs	Sig
		Service		through third-party services like social media platforms	Monitoring	
Persistence	T1547 - Boot or Logon Autostart Execution	T1547.001 - Registry Run Keys / Startup Folder	**High**	Monitor modifications to registry run keys and startup folder additions	Windows Registry Monitoring, Sysmon Event ID 13, File System Monitoring	
Persistence	T1547 - Boot or Logon Autostart Execution	T1547.003 - Time Providers	**Medium**	Monitor changes to time provider configurations	Registry Monitoring, System Configuration Logs	
Persistence	T1547 - Boot or Logon Autostart Execution	T1547.004 - Winlogon Helper DLL	**High**	Monitor winlogon registry modifications	Registry Monitoring, Sysmon Event ID 13	
Persistence	T1547 - Boot or Logon Autostart Execution	T1547.009 - Shortcut Modification	**Medium**	Monitor for changes to shortcut files (.lnk) in startup locations	File System Monitoring, Sysmon Event ID 11	
Privilege Escalation	T1548 - Abuse Elevation Control Mechanism	T1548.002 - Bypass User Account Control	**High**	Monitor for UAC bypass techniques and unexpected elevation of privileges	Windows Security Logs, UAC Event Logs, Process Monitoring	
Defense Evasion	T1562 - Impair Defenses	T1562.001 - Disable or Modify Tools	**Critical**	Monitor attempts to disable or modify security tools like Windows Defender	Security Tool Logs, Registry Monitoring, Service Control Logs	
Credential Access	T1555 - Credentials from	T1555.001 - Keychain	**Critical**	Monitor access to credential storage mechanisms	Keychain Access Logs, Process Monitoring, API Call Monitoring	

MITRE Category	MITRE Technique	MITRE Sub-technique	Severity	Detection Rule	Technology Logs	Sig
	Password Stores					
Credential Access	T1555 - Credentials from Password Stores	T1555.003 - Credentials from Web Browsers	**Critical**	Monitor browser credential store access	Browser Logs, Process Monitoring, File Access Logs	
Discovery	T1082 - System Information Discovery	N/A	**Low**	Monitor for commands that gather system information (systeminfo, whoami, uname)	Command Line Auditing, Process Monitoring, System Logs	
Discovery	T1083 - File and Directory Discovery	N/A	**Low**	Monitor for file enumeration commands (dir, ls, find)	File System Monitoring, Command Line Auditing	
Discovery	T1135 - Network Share Discovery	N/A	**Medium**	Monitor for network share enumeration (net view, showmount)	Network Monitoring, SMB Logs, Command Line Auditing	
Lateral Movement	T1021 - Remote Services	T1021.001 - Remote Desktop Protocol	**High**	Monitor RDP connections and authentication events	Windows Security Logs (Event ID 4624, 4625), RDP Logs, Network Monitoring	
Lateral Movement	T1021 - Remote Services	T1021.002 - SMB/Windows Admin Shares	**Critical**	Monitor SMB connections and administrative share access	SMB Logs, Windows Security Logs, Network Monitoring	
Lateral Movement	T1021 - Remote Services	T1021.004 - SSH	**High**	Monitor SSH connections and authentication attempts	SSH Logs, Authentication Logs, Network Monitoring	
Collection	T1005 - Data from	N/A	**Critical**	Monitor for large file reads and data	File System Monitoring, Data Loss Prevention,	

MITRE Category	MITRE Technique	MITRE Sub-technique	Severity	Detection Rule	Technology Logs	Sig
	Local System			staging activities	Process Monitoring	
Exfiltration	T1041 - Exfiltration Over C2 Channel	N/A	**Critical**	Monitor for unusual outbound network traffic patterns	Network Monitoring, Firewall Logs, Proxy Logs, DNS Logs	
Impact	T1490 - Inhibit System Recovery	N/A	**Critical**	Monitor deletion of backup files and system recovery mechanisms	File System Monitoring, Backup System Logs, Windows Event Logs	
Impact	T1486 - Data Encrypted for Impact	N/A	**Critical**	Monitor for rapid file encryption activities and ransomware indicators	File System Monitoring, Process Monitoring, Entropy Analysis	

Detection Implementation Notes

Key Technology Requirements:

1. **Sysmon** - Essential for Windows process, network, and file monitoring
2. **Windows Event Logs** - Critical for authentication, security, and system events
3. **Command Line Auditing** - Required for detecting command execution techniques
4. **PowerShell Logging** - Must be enabled for PowerShell-based detections
5. **EDR/XDR Platforms** - Provide comprehensive behavioral analysis and correlation
6. **Network Monitoring** - Essential for lateral movement and C2 detection
7. **Linux Audit (auditd)** - Required for Unix/Linux environment monitoring

Configuration Recommendations:

- Enable PowerShell Script Block Logging (Event ID 4104)
- Configure Sysmon with comprehensive configuration file
- Enable process command line auditing in Windows
- Implement network segmentation monitoring
- Deploy endpoint detection and response (EDR) solutions

- Configure centralized log collection and correlation (SIEM)

Severity Assessment Methodology

The severity ratings were determined based on the following criteria for an environment with EDR/XDR, non-admin users, and centralized SIEM logging:

Critical Severity

- **PowerShell T1059.001**: Extremely powerful execution vector, bypasses many controls, enables fileless attacks and credential theft
- **Process Hollowing T1055.012**: Completely evades process-based detection, enables persistent malware execution
- **Spearphishing Attacks T1566.001/002**: Primary initial access vector, bypasses perimeter security, high success rate
- **Disable Security Tools T1562.001**: Directly defeats security controls, enables follow-on attacks
- **Credential Theft T1555.001/003**: Direct access to stored credentials, enables account takeover and lateral movement
- **VBA Macros T1059.005**: Common malware delivery mechanism, often bypasses email security
- **Network Device CLI T1059.008**: Infrastructure compromise, potential for network-wide impact
- **SMB Admin Shares T1021.002**: High-privilege lateral movement, often leads to domain compromise
- **Data Collection/Exfiltration T1005/T1041**: Direct business impact, data loss, regulatory issues
- **Ransomware Techniques T1490/T1486**: Business-critical impact, operational shutdown

High Severity

- **Most Process Injection T1055.x**: Evades detection but EDR behavioral analysis can catch some variants
- **Command Shell T1059.003**: Powerful execution but well-monitored in mature environments
- **JavaScript/JScript T1059.007**: Common attack vector but increasingly detected
- **Phishing via Services T1566.003**: Harder to detect than email-based phishing
- **Persistence Techniques T1547.x**: Establishes foothold but limited immediate impact
- **UAC Bypass T1548.002**: Privilege escalation but requires initial access
- **Remote Access T1021.001/004**: Lateral movement capabilities

Medium Severity

- **Advanced Process Injection T1055.005/008/009/011/015**: Sophisticated but difficult to execute, likely caught by EDR
- **AppleScript T1059.002**: Limited to macOS environments, less common
- **Python Scripts T1059.006**: Powerful but well-monitored in enterprise environments
- **Time Providers T1547.003**: Persistence but limited impact
- **Shortcut Modification T1547.009**: Low-impact persistence technique
- **Network Share Discovery T1135**: Reconnaissance with moderate impact

Low Severity

- **System/File Discovery T1082/T1083**: Basic reconnaissance, easily detected, minimal direct impact

References

- MITRE ATT&CK Framework
- Sysmon Configuration Guide
- PowerShell Logging Best Practices
- Windows Audit Policy