



A1

T1091 - Replication Through Removable Media
T1078.003 - Valid Accounts: Local Accounts
T1200 - Hardware Additions
T1007 - System Service Discovery

A2

T1557 - Adversary-in-the-Middle
T1217 - Browser Information Discovery
T1134 - Access Token Manipulation

A3

T1542.005 - Pre-OS Boot: TFTP Boot
T1548.003 - Abuse Elevation Control Mechanism: Sudo and Sudo Caching
T1040 - Network Sniffing

A4

T1005 - Data from Local System
T1020.001 - Automated Exfiltration: Traffic Duplication

A5

T1486 - Data Encrypted for Impact

Reconnaissance 10 techniques	Resource Development 8 techniques	Initial Access 10 techniques	Execution 14 techniques	Persistence 20 techniques	Privilege Escalation 14 techniques	Defense Evasion 43 techniques	Credential Access 17 techniques	Discovery 32 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 17 techniques	Exfiltration 9 techniques	Impact 14 techniques
Active Scanning (0/3)	Acquire Access (0/3)	Content Injection (0/3)	Cloud Administration Command (0/3)	Account Manipulation (0/3)	Abuse Elevation Control Mechanism (0/3)	Abuse Elevation Control Mechanism (0/3)	Adversary-in-the-Middle (0/3)	Account Discovery (0/3)	Exploitation of Remote Services (0/3)	Adversary-in-the-Middle (0/3)	Application Layer Protocol (0/3)	Automated Exfiltration (0/3)	Account Access Removal (0/3)
Gather Victim Host Information (0/3)	Acquire Infrastructure (0/3)	Drive-by-Compromise (0/3)	Command and Scripting Interpreter (0/3)	BITS Jobs (0/3)	Access Token Manipulation (0/3)	Access Token Manipulation (0/3)	Brute Force (0/3)	Application Window Discovery (0/3)	Internal Spearphishing (0/3)	Archive Collected Data (0/3)	Communication Through Removable Media (0/3)	Data Transfer Size Limits (0/3)	Data Destruction (0/3)
Gather Victim Identity Information (0/3)	Compromise Accounts (0/3)	Exploit Public-Facing Application (0/3)	Container Administration Command (0/3)	Boot or Logon Autostart Execution (0/14)	Account Manipulation (0/3)	BITS Jobs (0/3)	Credentials from Password Stores (0/3)	Browser Information Discovery (0/3)	Lateral Tool Transfer (0/3)	Audio Capture (0/3)	Content Injection (0/3)	Exfiltration Over Alternative Protocol (0/3)	Data Encrypted for Impact (0/3)
Gather Victim Network Information (0/3)	Compromise Infrastructure (0/3)	External Remote Services (0/3)	Deploy Container (0/3)	Boot or Logon Initialization Scripts (0/3)	Account Manipulation (0/3)	Build Image on Host (0/3)	Exploitation for Credential Access (0/3)	Cloud Infrastructure Discovery (0/3)	Remote Service Session Hijacking (0/3)	Automated Collection (0/3)	Data Encoding (0/3)	Exfiltration Over C2 Channel (0/3)	Data Manipulation (0/3)
Gather Victim Org Information (0/3)	Develop Capabilities (0/3)	Hardware Additions (0/3)	Exploitation for Client Execution (0/3)	Browser Extensions (0/3)	Boot or Logon Autostart Execution (0/14)	Debugger Evasion (0/3)	Forced Authentication (0/3)	Cloud Service Dashboard (0/3)	Remote Services (0/3)	Browser Session Hijacking (0/3)	Data Obfuscation (0/3)	Defacement (0/3)	Defacement (0/3)
Phishing for Information (0/3)	Establish Accounts (0/3)	Phishing (0/3)	Inter-Process Communication (0/3)	Compromise Client Software Binary (0/3)	Boot or Logon Initialization Scripts (0/3)	Deploy Container (0/3)	Forge Web Credentials (0/3)	Cloud Storage Object Discovery (0/3)	Replication Through Removable Media (0/3)	Clipboard Data (0/3)	Dynamic Resolution (0/3)	Exfiltration Over Other Network Medium (0/3)	Disk Wipe (0/3)
Search Closed Sources (0/3)	Obtain Capabilities (0/3)	Replication Through Removable Media (0/3)	Native API (0/3)	Create Account (0/3)	Create or Modify System Process (0/3)	Direct Volume Access (0/3)	Input Capture (0/3)	Container and Resource Discovery (0/3)	Software Deployment Tools (0/3)	Data from Cloud Storage (0/3)	Encrypted Channel (0/3)	Exfiltration Over Physical Medium (0/3)	Financial Theft (0/3)
Search Open Technical Databases (0/3)	Stage Capabilities (0/3)	Supply Chain Compromise (0/3)	Scheduled Task/Job (0/3)	Create or Modify System Process (0/3)	Domain Policy Modification (0/3)	Domain Policy Modification (0/3)	Modify Authentication Process (0/3)	Debugger Evasion (0/3)	Taint Shared Content (0/3)	Data from Configuration Repository (0/3)	Fallback Channels (0/3)	Exfiltration Over Web Service (0/3)	Firmware Corruption (0/3)
Search Open Websites/Domains (0/3)	Trusted Relationship (0/3)	Valid Accounts (0/4)	Serverless Execution (0/3)	Event Triggered Execution (0/16)	Escape to Host (0/3)	Execution Guardrails (0/1)	Multi-Factor Authentication Request Interception (0/3)	Device Driver Discovery (0/3)	Use Alternate Authentication Material (0/3)	Data from Information Repositories (0/3)	Ingress Tool Transfer (0/3)	Scheduled Transfer (0/3)	Inhibit System Recovery (0/3)
Search Victim-Owned Websites (0/3)			Shared Modules (0/3)	External Remote Services (0/3)	Exploitation for Privilege Escalation (0/3)	File and Directory Permissions Modification (0/3)	Multi-Factor Authentication Request Interception (0/3)	Domain Trust Discovery (0/3)		Data from Network Shared Drive (0/3)	Non-Standard Port (0/3)	Transfer Data to Cloud Account (0/3)	Resource Hijacking (0/3)
			Software Deployment Tools (0/3)	Hijack Execution Flow (0/12)	Hide Artifacts (0/11)	Hide Artifacts (0/11)	Network Sniffing (0/3)	Log Enumeration (0/3)		Data from Removable Media (0/3)	Proxy (0/3)	System Shutdown/Reboot (0/3)	System Shutdown/Reboot (0/3)
			System Services (0/3)	Implant Internal Image (0/3)	Hijack Execution Flow (0/12)	Impair Defenses (0/11)	OS Credential Dumping (0/3)	Network Service Discovery (0/3)		Data Staged (0/3)	Remote Access Software (0/3)		
			User Execution (0/3)	Modify Authentication Process (0/3)	Process Injection (0/12)	Impersonation (0/11)	Steal Application Access Token (0/3)	Network Sniffing (0/3)		Email Collection (0/3)	Traffic Signaling (0/3)		
			Windows Management Instrumentation (0/3)	Office Application Startup (0/3)	Scheduled Task/Job (0/3)	Indicator Removal (0/3)	Steal or Forge Authentication Certificates (0/3)	Password Policy Discovery (0/3)		Input Capture (0/3)	Web Service (0/3)		
				Power Settings (0/3)	Valid Accounts (0/4)	Indirect Command Execution (0/3)	Steal or Forge Kerberos Tickets (0/3)	Peripheral Device Discovery (0/3)		Screen Capture (0/3)			
				Pre-OS Boot (0/3)		Masquerading (0/3)	Steal Web Session Cookie (0/3)	Permission Groups Discovery (0/3)		Video Capture (0/3)			
				Scheduled Task/Job (0/3)		Modify Authentication Process (0/3)	Unsecured Credentials (0/3)	Process Discovery (0/3)					
				Server Software Component (0/3)		Modify Cloud Compute Infrastructure (0/3)		Query Registry (0/3)					
				Traffic Signaling (0/3)		Modify Registry (0/3)		Remote System Discovery (0/3)					
						Modify System Image (0/3)		Software Discovery (0/3)					
						Network Boundary (0/3)		System Information (0/3)					

Красный – высокая опасность

Оранжевый – средняя опасность

Зеленый – низкая опасность

Угрозы:

T1091 - Replication Through Removable Media – красный

T1078.003 - Valid Accounts: Local Accounts – оранжевый

T1200 - Hardware Additions – красный

T1007 - System Service Discovery – оранжевый

T1557 - Adversary-in-the-Middle – красный

T1217 - Browser Information Discovery – зеленый

T1134 - Access Token Manipulation – зеленый

T1542.005 - Pre-OS Boot: TFTP Boot – оранжевый

T1548.003 - Abuse Elevation Control Mechanism: Sudo and Sudo Caching –
красный

T1040 - Network Sniffing – оранжевый

T1005 - Data from Local System – красный

T1020.001 - Automated Exfiltration: Traffic Duplication – оранжевый

T1486 - Data Encrypted for Impact – оранжевый