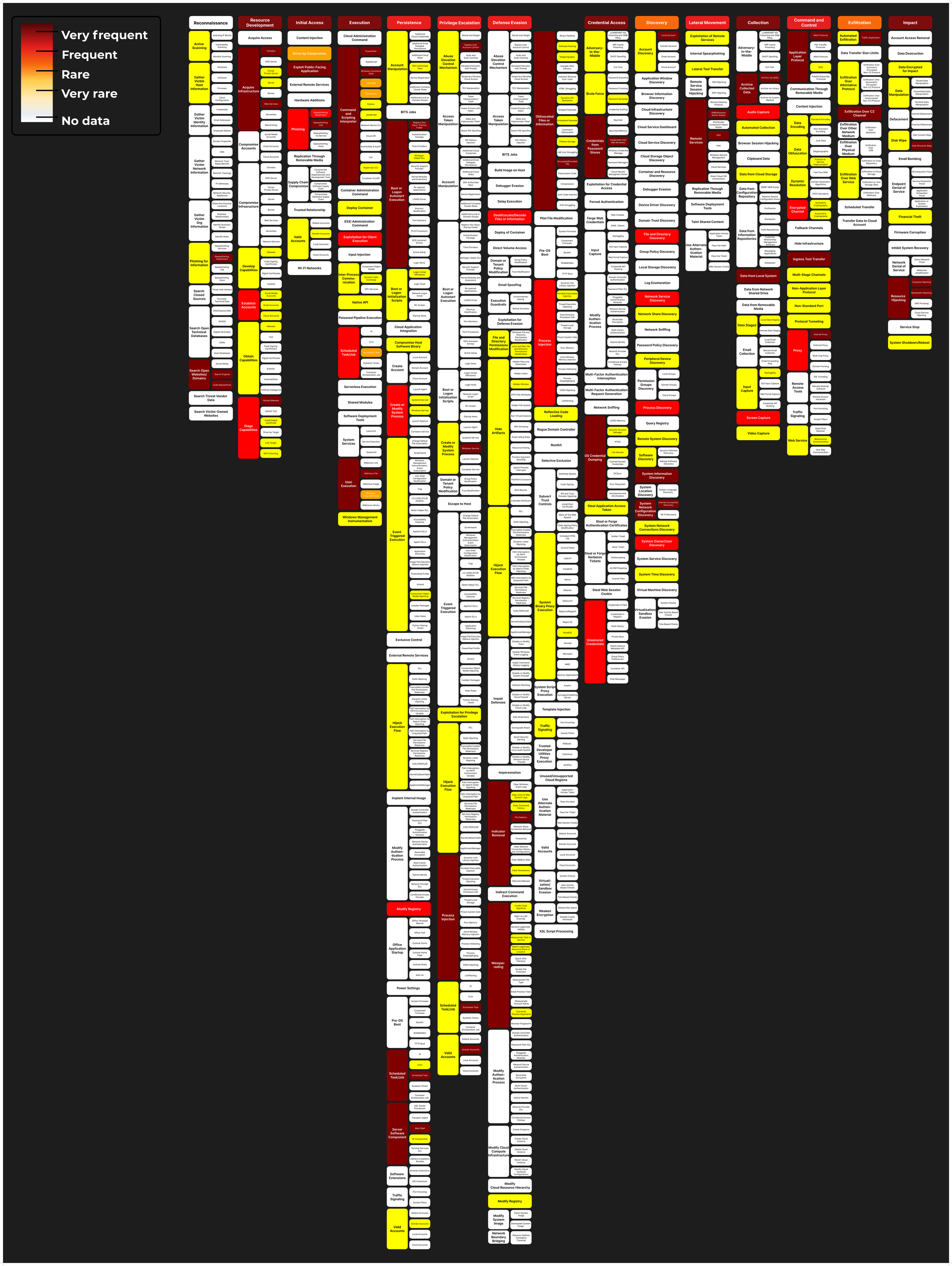
Very frequent
Frequent
Rare
Very rare
No data
Reconnaissance
Active Scanning
Scanning IP Blocks
Vulnerability Scanning
Wordlist Scanning
Gather Victim Host Information
Hardware
Software
Firmware
Client Configuration
Gather Victim Identity Information
Credentials
Email Addresses
Employee Names
Gather Victim Network Information
Domain Properties
DNS
Network Trust Dependencies
Network Topology
IP Addresses
Network Security Appliances
Gather Victim Org Information
Determine Physical Locations
Business Relationships
Identify Business Tempo
Identify Roles
Phishing for Information
Spearphishing Services
Spearphishing Attachment
Spearphishing Link
Spearphishing Voice
Search Closed Sources
Threat Intel Vendors
Purchase Technical Data
Search Open Technical Databases
DNS/Passive DNS
WHOIS
Digital Certicates
CDNs
Scan Databases
Social Media
Search Open Websites/ Domains
Search Engines
Code Repositories
Search Threat Vendor Data
Search Victim-Owned Websites
Resource Development
Acquire Access
Acquire Infrastructure
Domains
DNS Server
Virtual Private Server
Server
Botnet
Web Services
Serverless
Malvertising
Compromise Accounts
Social Media Accounts
Email Accounts
Cloud Accounts
Compromise Infrastructure
Domains
DNS Server
Virtual Private Server
Server
Botnet
Web Services
Serverless
Network Devices
Develop Capabilities
Malware
Code Signing Certificates
Digital Certificates
Exploits
Establish Accounts
Social Media Accounts
Email Accounts
Cloud Accounts
Obtain Capabilities
Malware
Tool
Code Signing Certificates
Digital Certificates
Exploits
Vulnerabilities
Artificial Intelligence
Stage Capabilities
Upload Malware
Upload Tool
Install Digital Certificate
Drive-by Target
Link Target
SEO Poisoning
Initial Access
Content Injection
Drive-by Compromise
Exploit Public-Facing Application
External Remote Services
Hardware Additions
Phishing
Spearphishing Attachment
Spearphishing Link
Spearphishing via Service
Spearphishing Voice
Replication Through Removable Media
Supply Chain Compromise
Compromise Software Dependencies and Development Tools
Compromise Software Supply Chain
Compromise Hardware Supply Chain
Trusted Relationship
Valid Accounts
Default Accounts
Domain Accounts
Local Accounts
Cloud Accounts
Wi-Fi Networks
Execution
Cloud Administration Command
Command and Scripting Interpreter
PowerShell
AppleScript
Windows Command Shell
Unix Shell
Visual Basic
Python
JavaScript
Network Device CLI
Cloud API
AutoHotKey & AutoIT
Lua
Hypervisor CLI
Container CLI/API
Container Administration Command
Deploy Container
ESXi Administration Command
Exploitation for Client Execution
Input Injection
Inter-Process Commu-nication
Component Object Model
Dynamic Data Exchange
XPC Services
Native API
Poisoned Pipeline Execution
Scheduled Task/Job
At
Cron
Scheduled Task
Systemd Timers
Container Orchestration Job
Serverless Execution
Shared Modules
Software Deployment Tools
System Services
Launchctl
Service Execution
Systemctl
User Execution
Malicious Link
Malicious File
Malicious Image
Malicious Copy and Paste
Malicious Library
Windows Management Instrumentation
Persistence
Account Manipulation
Additional Cloud Credentials
Additional Email Delegate Permissions
Additional Cloud Roles
SSH Authorized Keys
Device Registration
Additional Containe Cluster Roles
Additional Local or Domain Groups
BITS Jobs
Boot or Logon Autostart Execution
Registry Run Keys / Startup Folder
Authentication Package
Time Providers
Winlogon Helper DLL
Security Support Provider
Kernel Modules and Extensions
Re-opened Applications
LSASS Driver
Shortcut Modification
Port Monitors
Print Processors
XDG Autostart Entries
Active Setup
Login Items
Logon Script (Windows)
Login Hook
Network Logon Script
RC Scripts
Startup Items
Boot or Logon Initialization Scripts
Cloud Application Integration
Compromise Host Software Binary
Create Account
Local Account
Domain Account
Cloud Account
Create or Modify System Process
Launch Agent
Systemd Service
Windows Service
Launch Daemon
Container Service
Event Triggered Execution
Change Default File Association
Screensaver
Windows Management Instrumentation Event Subscription
Unix Shell Configuration Modification
Trap
LC_LOAD_DYLIB Addition
Netsh Helper DLL
Accessibility Features
AppCert DLLs
AppInit DLLs
Application Shimming
Image File Execution Options Injection
PowerShell Profile
Emond
Component Object Model Hijacking
Installer Packages
Udev Rules
Python Startup Hooks
Exclusive Control
External Remote Services
Hijack Execution Flow
DLL
Dylib Hijacking
Executable Installer File Permissions Weakness
Dynamic Linker Hijacking
Path Interception by PATH Environment Variable
Path Interception by Search Order Hijacking
Path Interception by Unquoted Path
Services File Permissions Weakness
Services Registry Permissions Weakness
COR_PROFILER
KernelCallbackTable
AppDomainManager
Implant Internal Image
Modify Authen-tication Process
Domain Controller Authentication
Password Filter DLL
Pluggable Authentication Modules
Network Device Authentication
Reversible Encryption
Multi-Factor Authentication
Hybrid Identity
Network Provider DLL
Conditional Access Provider
Modify Registry
Office Application Startup
Office Template Macros
Office Test
Outlook Forms
Outlook Home Page
Outlook Rules
Add-ins
Power Settings
Pre-OS Boot
System Firmware
Component Firmware
Bootkit
ROMMONkit
TFTP Boot
Scheduled Task/Job
At
Cron
Scheduled Task
Systemd Timers
Container Orchestration Job
Server Software Component
SQL Stored Procedures
Transport Agent
Web Shell
IIS Components
Terminal Services DLL
vSphere Installation Bundles
Software Extensions
Browser Extensions
IDE Extensions
Traffic Signaling
Port Knocking
Socket Filters
Valid Accounts
Default Accounts
Domain Accounts
Local Accounts
Cloud Accounts
Privilege Escalation
Abuse Elevation Control Mechanism
Setuid and Setgid
Bypass User Account Control
Sudo and Sudo Caching
Elevated Execution with Prompt
Temporary Elevated Cloud Access
TCC Manipulation
Access Token Manipulation
Token Impersonation/ Theft
Create Process with Token
Make and Impersonate Token
Parent PID Spoofing
SID-History Injection
Account Manipulation
Additional Cloud Credential
Additional Email Delegate Permissions
Additional Cloud Roles
SSH Authorized Keys
Device Registration
Additional Container Cluster Roles
Additional Local or Domain Groups
Boot or Logon Autostart Execution
Registry Run Keys/ Startup Folder
Authentication Package
Time Providers
Winlogon Helper DLL
Security Support Provider
Kernel Modules and Extensions
Re-opened Applications
LSASS Driver
Shortcut Modification
Port Monitors
Print Processors
XDG Autostart Entries
Active Setup
Login Items
Boot or Logon Initialization Scripts
Logon Script (Windows)
Login Hook
Network Logon Script
RC Scripts
Startup Items
Create or Modify System Process
Launch Agent
Systemd Service
Windows Service
Launch Daemon
Container Service
Domain or Tenant Policy Modification
Group Policy Modification
Trust Modification
Escape to Host
Event Triggered Execution
Change Default File Association
Screensaver
Windows Management Instrumentation Event Subscription
Unix Shell Configuration Modification
Trap
LC_LOAD_DYLIB Addition
Netsh Helper DLL
Accessibility Features
AppCert DLLs
AppInit DLLs
Application Shimming
Image File Execution Options Injection
PowerShell Profile
Emond
Component Object Model Hijacking
Installer Packages
Udev Rules
Python Startup Hooks
Exploitation for Privilege Escalation
Hijack Execution Flow
DLL
Dylib Hijacking
Executable Installer File Permissions Weakness
Dynamic Linker Hijacking
Path Interception by PATH Environment Variable
Path Interception by Search Order Hijacking
Path Interception by Unquoted Path
Services File Permissions Weakness
Services Registry Permissions Weakness
COR_PROFILER
KernelCallbackTable
AppDomainManager
Process Injection
Dynamic-link Library Injection
Portable Executable Injection
Thread Execution Hijacking
Asynchronous Procedure Call
Thread Local Storage
Ptrace System Calls
Proc Memory
Extra Window Memory Injection
Process Hollowing
Process Doppelgänging
VDSO Hijacking
ListPlanting
Scheduled Task/Job
At
Cron
Scheduled Task
Systemd Timers
Container Orchestration Job
Valid Accounts
Default Accounts
Domain Accounts
Local Accounts
Cloud Accounts
Defense Evasion
Abuse Elevation Control Mechanism
Setuid and Setgid
Bypass User Account Control
Sudo and Sudo Caching
Elevated Execution with Prompt
Temporary Elevated Cloud Access
TCC Manipulation
Access Token Manipulation
Token Impersonation/ Theft
Create Process with Token
Make and Impersonate Token
Parent PID Spoofing
SID-History Injection
BITS Jobs
Build Image on Host
Debugger Evasion
Delay Execution
Deobfuscate/Decode Files or Information
Deploy of Container
Direct Volume Access
Domain or Tenant Policy Modification
Group Policy Modification
Trust Modification
Email Spoofing
Execution Guardrails
Environmental Keying
Mutual Exclusion
Exploitation for Defense Evasion
File and Directory Permissions Modification
Windows File and Directory Permissions Modification
Linux and Mac File and Directory Permissions Modification
Hide Artifacts
Hidden Files and Directories
Hidden Users
Hidden Window
NTFS File Attributes
Hidden File System
Run Virtual Instance
VBA Stomping
Email Hiding Rules
Resource Forking
Process Argument Spoofing
Ignore Process Interrupts
File/Path Exclusions
Bind Mounts
Extended Attributes
Hijack Execution Flow
DLL
Dylib Hijacking
Executable Installer File Permissions Weakness
Dynamic Linker Hijacking
Path Interception by PATH Environment Variable
Path Interception by Search Order Hijacking
Path Interception by Unquoted Path
Services File Permissions Weakness
Services Registry Permissions Weakness
COR_PROFILER
KernelCallbackTable
AppDomainManager
Impair Defenses
Disable or Modify Tools
Disable Windows Event Logging
Impair Command History Logging
Disable or Modify System Firewall
Indicator Blocking
Disable or Modify Cloud Firewall
Disable or Modify Cloud Logs
Safe Mode Boot
Downgrade Attack
Spoof Security Alerting
Disable or Modify Linux Audit System
Disable or Modify Network Device Firewall
Impersonation
Indicator Removal
Clear Windows Event Logs
Clear Linux or Mac System Logs
Clear Command History
File Deletion
Network Share Connection Removal
Timestomp
Clear Network Connection History and Configurations
Clear Mailbox Data
Clear Persistence
Relocate Malware
Indirect Command Execution
Masque-rading
Invalid Code Signature
Right-to-Left Override
Rename Legitimate Utilities
Masquerade Task or Service
Match Legitimate Resource Name or Location
Space after Filename
Double File Extension
Masquerade File Type
Break Process Trees
Masquerade Account Name
Overwrite Process Arguments
Browser Fingerprint
Modify Authen-tication Process
Domain Controller Authentication
Password Filter DLL
Pluggable Authentication Modules
Network Device Authentication
Reversible Encryption
Multi-Factor Authentication
Hybrid Identity
Network Provider DLL
Conditional Access Policies
Modify Cloud Compute Infrastructure
Create Snapshot
Create Cloud Instance
Delete Cloud Instance
Revert Cloud Instance
Modify Cloud Compute Configurations
Modify Cloud Resource Hierarchy
Modify Registry
Modify System Image
Patch System Image
Downgrade System Image
Network Boundary Bridging
Network Address Translation Traversal
Obfuscated Files or Information
Binary Padding
Software Packing
Steganography
Compile After Delivery
Indicator Removal from Tools
HTML Smuggling
Dynamic API Resolution
Stripped Payloads
Embedded Payloads
Command Obfuscation
Fileless Storage
LNK Icon Smuggling
Encrypted/Encoded File
Polymorphic Code
Compression
Junk Code Insertion
SVG Smuggling
Plist File Modification
Pre-OS Boot
System Firmware
Component Firmware
Bootkit
ROMMONkit
TFTP Boot
Process Injection
Dynamic-link Library Injection
Portable Executable Injection
Thread Execution Hijacking
Asynchronous Procedure Call
Thread Local Storage
Ptrace System Calls
Proc Memory
Extra Window Memory Injection
Process Hollowing
Process Doppelgänging
VDSO Hijacking
ListPlanting
Reflective Code Loading
Rogue Domain Controller
Rootkit
Selective Exclusion
Subvert Trust Controls
Gatekeep Bypass
Code Signing
SIP and Trust Provider Hijacking
Install Root Certificate
Mark-of-the-Web Bypass
Code Signing Policy Modification
System Binary Proxy Execution
Compiled HTML File
Control Panel
CMSTP
InstallUtil
Mshta
Msiexec
Obdcconf
Regsvcs/Regasm
Regsvr32
Rundll32
Verclsid
Mavinject
MMC
Electron Applications
System Script Proxy Execution
PubPrn
SyncAppvPublishing Server
Template Injection
Traffic Signaling
Port Knocking
Socket Filters
Trusted Developer Utilities Proxy Execution
MSBuild
ClickOnce
JamPlus
Unused/Unsupported Cloud Regions
Use Alternate Authen-tication Material
Application Access Token
Pass the Hash
Pass the Ticket
Web Session Cookie
Valid Accounts
Default Accounts
Domain Accounts
Local Accounts
Cloud Accounts
Virtuali-zation/ Sandbox Evasion
System Checks
User Activity Based Checks
Time Based Checks
Weaken Encryption
Reduce Key Space
Disable Crypto Hardware
XSL Script Processing
Credential Access
Adversary-in-the-Middle
LLMNR/NBT-NS Poisoning and SMB Relay
ARP Cache Poisoning
DHCP Spoofing
Evil Twin
Brute Force
Password Guessing
Password Cracking
Password Spraying
Credential Stuffing
Credentials from Password Stores
Keychain
Securityd Memory
Credentials from Web Browsers
Windows Credential Manager
Password Managers
Cloud Secrets Management Stores
Exploitation for Credential Access
Forced Authentication
Forge Web Credentials
Web Cookies
SAML Tokens
Input Capture
Keylogging
GUI Input Capture
Web Portal Capture
Credential API Hooking
Modify Authen-tication Process
Domain Controller Authentication
Password Filter DLL
Pluggable Authentication Modules
Network Device Authentication
Reversible Encryption
Multi-Factor Authentication
Hybrid Identity
Network Provider DLL
Conditional Access Policies
Multi-Factor Authentication Interception
Multi-Factor Authentication Request Generation
Network Sniffing
OS Credential Dumping
LSASS Memory
Security Account Manager
NTDS
LSA Secrets
Cached Domain Credentials
DCSync
Proc Filesystem
/etc/passwd and /etc/shadow
Steal Application Access Token
Steal or Forge Authentication Certificates
Steal or Forge Kerberos Tickets
Golden Ticket
Silver Ticket
Kerberoasting
AS-REP Roasting
Ccache Files
Steal Web Session Cookie
Unsecured Credentials
Credentials in Files
Credentials in Registry
Shell History
Private Keys
Cloud Instance Metadata API
Group Policy Preferences
Container API
Chat Messages
Discovery
Account Discovery
Local Account
Domain Account
Email Account
Cloud Account
Application Window Discovery
Browser Information Discovery
Cloud Infrastructure Discovery
Cloud Service Dashboard
Cloud Service Discovery
Cloud Storage Object Discovery
Container and Resource Discovery
Debugger Evasion
Device Driver Discovery
Domain Trust Discovery
File and Directory Discovery
Group Policy Discovery
Local Storage Discovery
Log Enumeration
Network Service Discovery
Network Share Discovery
Network Sniffing
Password Policy Discovery
Peripheral Device Discovery
Permission Groups Discovery
Local Groups
Domain Groups
Cloud Groups
Process Discovery
Query Registry
Remote System Discovery
Software Discovery
Security Software Discovery
Backup Software Discovery
System Information Discovery
System Location Discovery
System Language Discovery
System Network Configuration Discovery
Internet Connection Discovery
Wi-Fi Discovery
System Network Connections Discovery
System Owner/User Discovery
System Service Discovery
System Time Discovery
Virtual Machine Discovery
Virtualization/ Sandbox Evasion
System Checks
User Activity Based Checks
Time Based Checks
Lateral Movement
Exploitation of Remote Services
Internal Spearphishing
Lateral Tool Transfer
Remote Service Session Hijacking
SSH Hijacking
RDP Hijacking
Remote Services
Remote Desktop Protocol
SMB/Windows Admin Shares
Distributed Component Object Model
SSH
VNC
Windows Remote Management
Cloud Services
Direct Cloud VM Connections
Replication Through Removable Media
Software Deployment Tools
Taint Shared Content
Use Alternate Authen-tication Material
Application Access Token
Pass the Hash
Pass the Ticket
Web Session Cookie
Collection
Adversary-in-the-Middle
LLMNR/NBT-NS Poisoning and SMB Relay
ARP Cache Poisoning
DHCP Spoofing
Evil Twin
Archive Collected Data
Archive via Utility
Archive via Library
Archive via Custom Method
Audio Capture
Automated Collection
Browser Session Hijacking
Clipboard Data
Data from Cloud Storage
Data from Configuration Repository
SNMP (MIB Dump)
Network Device Configuration Dump
Data from Information Repositories
Confluence
Sharepoint
Code Repositories
Customer Relationship Management Software
Messaging Applications
Databases
Data from Local System
Data from Network Shared Drive
Data from Removable Media
Data Staged
Local Data Staging
Remote Data Staging
Email Collection
Local Email Collection
Remote Email Collection
Email Forwarding Rule
Input Capture
Keylogging
GUI Input Capture
Web Portal Capture
Credential API Hooking
Screen Capture
Video Capture
Command and Control
Application Layer Protocol
Web Protocols
File Transfer Protocols
Mail Protocols
DNS
Publish/Subscribe Protocols
Communication Through Removable Media
Content Injection
Data Encoding
Standard Encoding
Non-Standard Encoding
Data Obfuscation
Junk Data
Steganography
Protocol or Service Impersonation
Dynamic Resolution
Fast Flux DNS
Domain Generation Algorithms
DNS Calculation
Encrypted Channel
Symmetric Cryptography
Asymmetric Cryptography
Fallback Channels
Hide Infrastructure
Ingress Tool Transfer
Multi-Stage Channels
Non-Application Layer Protocol
Non-Standard Port
Protocol Tunneling
Proxy
Internal Proxy
External Proxy
Multi-hop Proxy
Domain Fronting
Remote Access Tools
IDE Tunneling
Remote Desktop Software
Remote Access Hardware
Traffic Signaling
Port Knocking
Socket Filters
Web Service
Dead Drop Resolver
Bidirectional Communication
One-Way Communication
Exfiltration
Automated Exfiltration
Traffic Duplication
Data Transfer Size Limits
Exfiltration Over Alternative Protocol
Exfiltration Over Symmetric Encrypted Non-C2 Protocol
Exfiltration Over Asymmetric Encrypted Non-C2 Protocol
Exfiltration Over Unencrypted Non-C2 Protocol
Exfiltration Over C2 Channel
Exfiltration Over Other Network Medium
Exfiltration Over Bluetooth
Exfiltration Over Physical Medium
Exfiltration Over USB
Exfiltration Over Web Service
Exfiltration to Code Repository
Exfiltration to Cloud Storage
Exfiltration to Text Storage Sites
Exfiltration Over Webhook
Scheduled Transfer
Transfer Data to Cloud Account
Impact
Account Access Removal
Data Destruction
Data Encrypted for Impact
Data Manipulation
Stored Data Manipulation
Transmitted Data Manipulation
Runtime Data Manipulation
Defacement
Internal Defacement
External Defacement
Disk Wipe
Disk Content Wipe
Disk Structure Wipe
Email Bombing
Endpoint Denial of Service
OS Exhaustion Flood
Service Exhaustion Flood
Application Exhaustion Flood
Application or System Exploitation
Financial Theft
Firmware Corruption
Inhibit System Recovery
Network Denial of Service
Direct Network Flood
Reflection Amplification
Resource Hijacking
Compute Hijacking
Bandwidth Hijacking
SMS Pumping
Cloud Service Hijacking
Service Stop
System Shutdown/Reboot