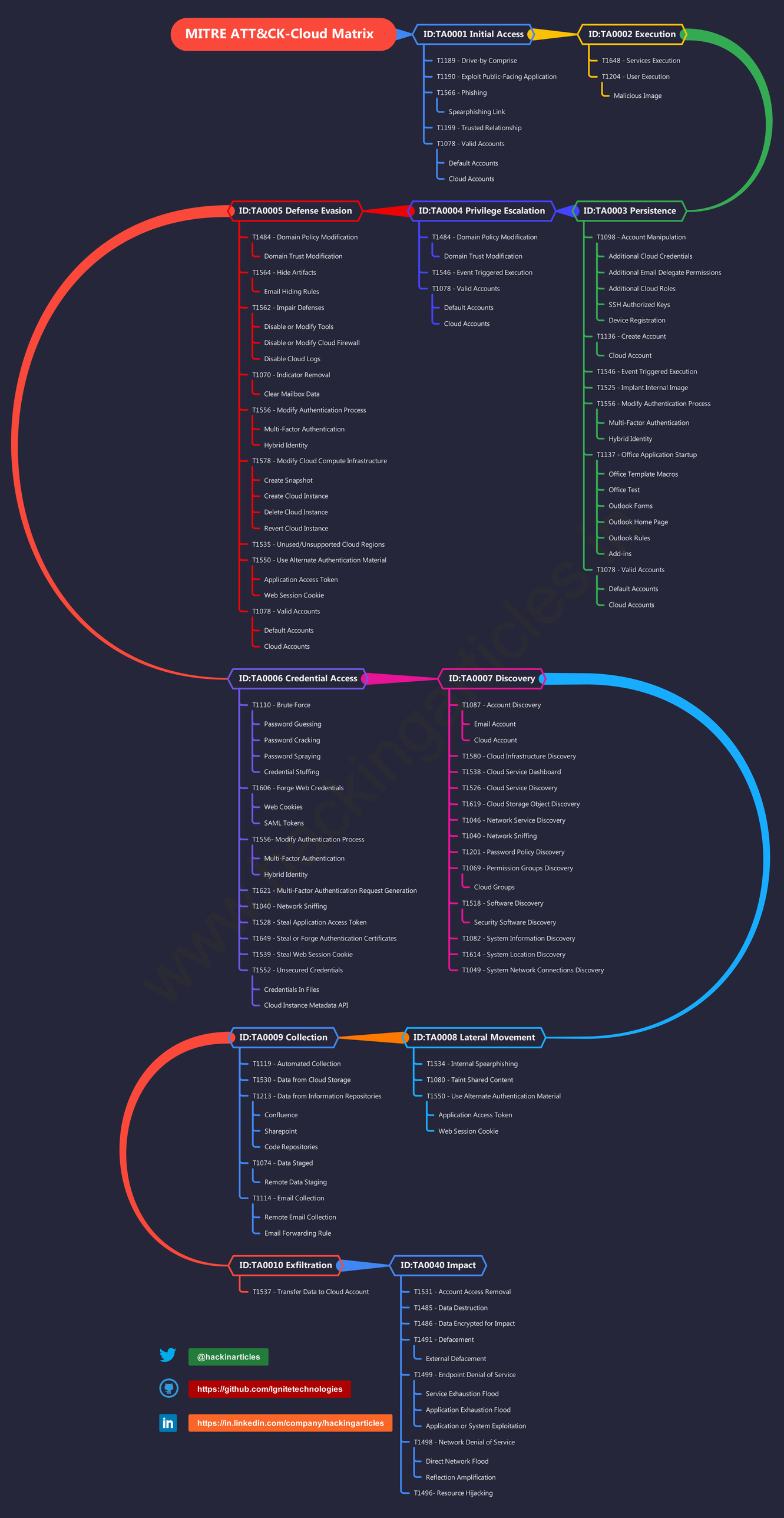
MITRE ATT&CK-Cloud Matrix
ID:TA0001 Initial Access
T1189 - Drive-by Comprise
T1190 - Exploit Public-Facing Application
T1566 - Phishing
Spearphishing Link
T1199 - Trusted Relationship
T1078 - Valid Accounts
Default Accounts
Cloud Accounts
ID:TA0002 Execution
T1648 - Services Execution
T1204 - User Execution
Malicious Image
ID:TA0003 Persistence
T1098 - Account Manipulation
Additional Cloud Credentials
Additional Email Delegate Permissions
Additional Cloud Roles
SSH Authorized Keys
Device Registration
T1136 - Create Account
Cloud Account
T1546 - Event Triggered Execution
T1525 - Implant Internal Image
T1556 - Modify Authentication Process
Multi-Factor Authentication
Hybrid Identity
T1137 - Office Application Startup
Office Template Macros
Office Test
Outlook Forms
Outlook Home Page
Outlook Rules
Add-ins
T1078 - Valid Accounts
Default Accounts
Cloud Accounts
ID:TA0004 Privilege Escalation
T1484 - Domain Policy Modification
Domain Trust Modification
T1546 - Event Triggered Execution
T1078 - Valid Accounts
Default Accounts
Cloud Accounts
ID:TA0005 Defense Evasion
T1484 - Domain Policy Modification
Domain Trust Modification
T1564 - Hide Artifacts
Email Hiding Rules
T1562 - Impair Defenses
Disable or Modify Tools
Disable or Modify Cloud Firewall
Disable Cloud Logs
T1070 - Indicator Removal
Clear Mailbox Data
T1556 - Modify Authentication Process
Multi-Factor Authentication
Hybrid Identity
T1578 - Modify Cloud Compute Infrastructure
Create Snapshot
Create Cloud Instance
Delete Cloud Instance
Revert Cloud Instance
T1535 - Unused/Unsupported Cloud Regions
T1550 - Use Alternate Authentication Material
Application Access Token
Web Session Cookie
T1078 - Valid Accounts
Default Accounts
Cloud Accounts
ID:TA0006 Credential Access
T1110 - Brute Force
Password Guessing
Password Cracking
Password Spraying
Credential Stuffing
T1606 - Forge Web Credentials
Web Cookies
SAML Tokens
T1556- Modify Authentication Process
Multi-Factor Authentication
Hybrid Identity
T1621 - Multi-Factor Authentication Request Generation
T1040 - Network Sniffing
T1528 - Steal Application Access Token
T1649 - Steal or Forge Authentication Certificates
T1539 - Steal Web Session Cookie
T1552 - Unsecured Credentials
Credentials In Files
Cloud Instance Metadata API
ID:TA0007 Discovery
T1087 - Account Discovery
Email Account
Cloud Account
T1580 - Cloud Infrastructure Discovery
T1538 - Cloud Service Dashboard
T1526 - Cloud Service Discovery
T1619 - Cloud Storage Object Discovery
T1046 - Network Service Discovery
T1040 - Network Sniffing
T1201 - Password Policy Discovery
T1069 - Permission Groups Discovery
Cloud Groups
T1518 - Software Discovery
Security Software Discovery
T1082 - System Information Discovery
T1614 - System Location Discovery
T1049 - System Network Connections Discovery
ID:TA0008 Lateral Movement
T1534 - Internal Spearphishing
T1080 - Taint Shared Content
T1550 - Use Alternate Authentication Material
Application Access Token
Web Session Cookie
ID:TA0009 Collection
T1119 - Automated Collection
T1530 - Data from Cloud Storage
T1213 - Data from Information Repositories
Confluence
Sharepoint
Code Repositories
T1074 - Data Staged
Remote Data Staging
T1114 - Email Collection
Remote Email Collection
Email Forwarding Rule
ID:TA0010 Exfiltration
T1537 - Transfer Data to Cloud Account
ID:TA0040 Impact
T1531 - Account Access Removal
T1485 - Data Destruction
T1486 - Data Encrypted for Impact
T1491 - Defacement
External Defacement
T1499 - Endpoint Denial of Service
Service Exhaustion Flood
Application Exhaustion Flood
Application or System Exploitation
T1498 - Network Denial of Service
Direct Network Flood
Reflection Amplification
T1496- Resource Hijacking
@hackinarticles
https://github.com/Ignitetechnologies
https://in.linkedin.com/company/hackingarticles