MITRE ATT&CK / iOS Matrix

ID:TA0034 Impact
- T1642 Endpoint Denial of Service
- T1643 Generate Traffic from Victim
- T1464 Network Denial of Service

ID:TA0036 Exfiltration
- Exfiltration Over Unencrypted Non-C2 Protocol
- T1639 Exfiltration Over Alternative Protocol
- T1646 Exfiltration Over C2 Channel

ID:TA0037 Command and Control
- Web Protocols
- T1437 Application Layer Protocol
- Domain Generation Algorithms
- T1637 Dynamic Resolution
- Symmetric Cryptography
- Asymmetric Cryptography
- T1521 Encrypted Channel
- T1544 Ingress Tool Transfer
- T1509 Non-Standard Port
- T1644 Out of Band Data
- Dead Drop Resolver
- Bidirectional Communication
- T1481 Web Service
- One-Way Communication

ID:TA0035 Collection
- T1638 Adversary-in-the-Middle
- T1532 Archive Collected Data
- T1429 Audio Capture
- T1414 Clipboard Data
- T1533 Data from Local System
- Keylogging
- GUI Input Capture
- T1417 Input Capture
- Remote Device Management Services
- Impersonate SS7 Nodes
- T1430 Location Tracking
- Calendar Entries
- Call Log
- Contact List
- SMS Messages
- T1636 Protected User Data
- T1409 Stored Application Data
- T1512 Video Capture

ID:TA0033 Lateral Movement
- T1428 Exploitation of Remote Services
- T1458 Replication Through Removable Media

ID:TA0032 Discovery
- T1420 File and Directory Discovery
- Remote Device Management Services
- Impersonate SS7 Nodes
- T1430 Location Tracking
- T1423 Network Service Scanning
- T1424 Process Discovery
- Security Software Discovery
- T1418 Software Discovery
- T1426 System Information Discovery
- T1422 System Network Configuration Discovery

ID:TA0027 Initial Access
- T1456 Drive-By Compromise
- T1461 Lockscreen Bypass
- T1458 Replication Through Removable Media
- T1474 Supply Chain Compromise
  - Compromise Software Dependencies and Development Tools
  - Compromise Hardware Supply Chain
  - Compromise Software Supply Chain

ID:TA0041 Execution
- T1623 Command and Scripting Interpreter
  - Unix Shell
- T1603 Scheduled Task/Job

ID:TA0028 Persistence
- T1398 Boot or Logon Initialization Scripts
- T1645 Compromise Client Software Binary
- T1603 Scheduled Task/Job

ID:TA0029 Privilege Escalation
- T1404 Exploitation for Privilege Escalation
- T1631 Process Injection
  - Ptrace System Calls

ID:TA0030 Defense Evasion
- T1407 Download New Code at Runtime
- T1627 Execution Guardrails
  - Geofencing
- T1630 Indicator Removal on Host
  - Disguise Root/Jailbreak Indicators
- T1406 Obfuscated Files or Information
  - Software Packing
- T1631 Process Injection
  - Ptrace System Calls
- T1632 Subvert Trust Controls
  - Code Signing Policy Modification
- T1633 Virtualization/Sandbox Evasion
  - System Checks

ID:TA0031 Credential Access
- T1414 Clipboard Data
- T1634 Credentials from Password Store
  - Keychain
- T1417 Input Capture
  - Keylogging
  - GUI Input Capture
- T1635 Steal Application Access Token
  - URI Hijacking

www.hackingarticles.in

@hackinarticles
https://github.com/Ignitetechnologies
https://in.linkedin.com/company/hackingarticles