about

Hive

Capa con las tácticas y técnicas que usa el ransomware Hive.

Reconnaissance

- T1595: Active Scanning
- T1592: Gather Victim Host Information
- T1589: Gather Victim Identity Information
- T1590: Gather Victim Network Information
- T1591: Gather Victim Org Information
- T1598: Phishing for Information
- T1597: Search Closed Sources
- T1596: Search Open Technical Databases
- T1593: Search Open Websites/Domains
- T1594: Search Victim-Owned Websites

Resource Development

- T1583: Acquire Infrastructure
- T1586: Compromise Accounts
- T1584: Compromise Infrastructure
- T1587: Develop Capabilities
- T1585: Establish Accounts
- T1588: Obtain Capabilities
- T1608: Stage Capabilities

Initial Access

- T1189: Drive-by Compromise
- 🟥 T1190: Exploit Public-Facing Application
- 🟥 T1133: External Remote Services
- T1200: Hardware Additions
- T1566: Phishing
  - T1566.002: Spearphishing Link
  - T1566.003: Spearphishing via Service
  - 🟥 T1566.001: Spearphishing Attachment
- T1091: Replication Through Removable Media
- T1195: Supply Chain Compromise
- T1199: Trusted Relationship
- 🟥 T1078: Valid Accounts

Execution

- 🟥 T1059: Command and Scripting Interpreter
  - T1059.008: Network Device CLI
  - T1059.004: Unix Shell
  - T1059.002: AppleScript
  - 🟥 T1059.003: Windows Command Shell
  - T1059.005: Visual Basic
  - T1059.006: Python
  - 🟥 T1059.001: PowerShell
  - T1059.007: JavaScript
- T1609: Container Administration Command
- T1610: Deploy Container
- T1203: Exploitation for Client Execution
- T1559: Inter-Process Communication
- 🟥 T1106: Native API
- T1053: Scheduled Task/Job
- T1129: Shared Modules
- T1072: Software Deployment Tools
- T1569: System Services
- T1204: User Execution
- 🟥 T1047: Windows Management Instrumentation

Persistence

- 🟥 T1098: Account Manipulation
- 🟥 T1197: BITS Jobs
- T1547: Boot or Logon Autostart Execution
- T1037: Boot or Logon Initialization Scripts
- T1176: Browser Extensions
- T1554: Compromise Client Software Binary
- T1136: Create Account
- T1543: Create or Modify System Process
  - T1543.004: Launch Daemon
  - T1543.002: Systemd Service
  - 🟥 T1543.003: Windows Service
  - T1543.001: Launch Agent
- T1546: Event Triggered Execution
- 🟥 T1133: External Remote Services
- T1574: Hijack Execution Flow
- T1525: Implant Internal Image
- T1556: Modify Authentication Process
- T1137: Office Application Startup
- T1542: Pre-OS Boot
- T1053: Scheduled Task/Job
  - T1053.003: Cron
  - T1053.006: Systemd Timers
  - T1053.002: At
  - 🟥 T1053.005: Scheduled Task
  - T1053.007: Container Orchestration Job
- T1505: Server Software Component
- T1205: Traffic Signaling
- 🟥 T1078: Valid Accounts

Privilege Escalation

- T1548: Abuse Elevation Control Mechanism
- T1134: Access Token Manipulation
- T1547: Boot or Logon Autostart Execution
- T1037: Boot or Logon Initialization Scripts
- T1543: Create or Modify System Process
  - T1543.004: Launch Daemon
  - T1543.002: Systemd Service
  - 🟥 T1543.003: Windows Service
  - T1543.001: Launch Agent
- T1484: Domain Policy Modification
- T1611: Escape to Host
- T1546: Event Triggered Execution
- 🟥 T1068: Exploitation for Privilege Escalation
- T1574: Hijack Execution Flow
- 🟥 T1055: Process Injection
- T1053: Scheduled Task/Job
- 🟥 T1078: Valid Accounts

Defense Evasion

- T1548: Abuse Elevation Control Mechanism
- T1134: Access Token Manipulation
- 🟥 T1197: BITS Jobs
- T1612: Build Image on Host
- T1622: Debugger Evasion
- 🟥 T1140: Deobfuscate/Decode Files or Information
- T1610: Deploy Container
- T1006: Direct Volume Access
- T1484: Domain Policy Modification
- T1480: Execution Guardrails
- T1211: Exploitation for Defense Evasion
- T1222: File and Directory Permissions Modification
- T1564: Hide Artifacts
- T1574: Hijack Execution Flow
- T1562: Impair Defenses
- T1070: Indicator Removal on Host
  - T1070.002: Clear Linux or Mac System Logs
  - T1070.006: Timestomp
  - 🟥 T1070.004: File Deletion
  - 🟥 T1070.001: Clear Windows Event Logs
  - T1070.003: Clear Command History
  - T1070.005: Network Share Connection Removal
- T1202: Indirect Command Execution
- 🟥 T1036: Masquerading
- T1556: Modify Authentication Process
- T1578: Modify Cloud Compute Infrastructure
- T1112: Modify Registry
- T1601: Modify System Image
- T1599: Network Boundary Bridging
- T1027: Obfuscated Files or Information
- T1647: Plist File Modification
- T1542: Pre-OS Boot
- 🟥 T1055: Process Injection
- T1620: Reflective Code Loading
- T1207: Rogue Domain Controller
- T1014: Rootkit
- T1553: Subvert Trust Controls
- 🟥 T1218: System Binary Proxy Execution
- T1216: System Script Proxy Execution
- T1221: Template Injection
- T1205: Traffic Signaling
- T1127: Trusted Developer Utilities Proxy Execution
- T1535: Unused/Unsupported Cloud Regions
- T1550: Use Alternate Authentication Material
- 🟥 T1078: Valid Accounts
- T1497: Virtualization/Sandbox Evasion
- T1600: Weaken Encryption
- T1220: XSL Script Processing

Credential Access

- T1557: Adversary-in-the-Middle
- 🟥 T1110: Brute Force
- T1555: Credentials from Password Store
- T1212: Exploitation for Credential Access
- T1187: Forced Authentication
- T1606: Forge Web Credentials
- T1056: Input Capture
- T1556: Modify Authentication Process
- T1111: Multi-Factor Authentication Interception
- T1621: Multi-Factor Authentication Request Generation
- T1040: Network Sniffing
- 🟥 T1003: OS Credential Dumping
- T1528: Steal Application Access Token
- T1558: Steal or Forge Kerberos Tickets
- T1539: Steal Web Session Cookie
- T1552: Unsecured Credentials

Discovery

- 🟥 T1087: Account Discovery
- T1010: Application Window Discovery
- T1217: Browser Bookmark Discovery
- T1580: Cloud Infrastructure Discovery
- T1538: Cloud Service Dashboard
- T1526: Cloud Service Discovery
- T1619: Cloud Storage Object Discovery
- T1613: Container and Resource Discovery
- T1622: Debugger Evasion
- T1482: Domain Trust Discovery
- 🟥 T1083: File and Directory Discovery
- T1615: Group Policy Discovery
- T1046: Network Service Discovery
- 🟥 T1135: Network Share Discovery
- T1040: Network Sniffing
- T1201: Password Policy Discovery
- T1120: Peripheral Device Discovery
- T1069: Permission Groups Discovery
- 🟥 T1057: Process Discovery
- T1012: Query Registry
- 🟥 T1018: Remote System Discovery
- T1518: Software Discovery
- T1082: System Information Discovery
- T1614: System Location Discovery
- T1016: System Network Configuration Discovery
- 🟥 T1049: System Network Connections Discovery
- T1033: System Owner/User Discovery
- T1007: System Service Discovery
- T1124: System Time Discovery
- T1497: Virtualization/Sandbox Evasion

Lateral Movement

- T1210: Exploitation of Remote Services
- T1534: Internal Spearphishing
- 🟥 T1570: Lateral Tool Transfer
- T1563: Remote Service Session Hijacking
- T1021: Remote Services
  - T1021.003: Distributed Component Object Model
  - 🟥 T1021.002: SMB/Windows Admin Shares
  - T1021.004: SSH
  - T1021.005: VNC
  - 🟥 T1021.006: Windows Remote Management
  - 🟥 T1021.001: Remote Desktop Protocol
- T1091: Replication Through Removable Media
- T1072: Software Deployment Tools
- T1080: Taint Shared Content
- T1550: Use Alternate Authentication Material

Collection

- T1557: Adversary-in-the-Middle
- T1560: Archive Collected Data
  - 🟥 T1560.001: Archive via Utility
  - T1560.002: Archive via Library
  - T1560.003: Archive via Custom Method
- T1123: Audio Capture
- T1119: Automated Collection
- T1185: Browser Session Hijacking
- T1115: Clipboard Data
- T1530: Data from Cloud Storage Object
- T1602: Data from Configuration Repository
- T1213: Data from Information Repositories
- 🟥 T1005: Data from Local System
- T1039: Data from Network Shared Drive
- T1025: Data from Removable Media
- T1074: Data Staged
- T1114: Email Collection
- T1056: Input Capture
- T1113: Screen Capture
- T1125: Video Capture

Command and Control

- T1071: Application Layer Protocol
  - T1071.002: File Transfer Protocols
  - T1071.003: Mail Protocols
  - T1071.004: DNS
  - 🟥 T1071.001: Web Protocols
- T1092: Communication Through Removable Media
- T1132: Data Encoding
- T1001: Data Obfuscation
- T1568: Dynamic Resolution
- T1573: Encrypted Channel
- T1008: Fallback Channels
- T1105: Ingress Tool Transfer
- T1104: Multi-Stage Channels
- T1095: Non-Application Layer Protocol
- T1571: Non-Standard Port
- T1572: Protocol Tunneling
- T1090: Proxy
- T1219: Remote Access Software
- T1205: Traffic Signaling
- T1102: Web Service

Exfiltration

- T1020: Automated Exfiltration
- T1030: Data Transfer Size Limits
- T1048: Exfiltration Over Alternative Protocol
- 🟥 T1041: Exfiltration Over C2 Channel
- T1011: Exfiltration Over Other Network Medium
- T1052: Exfiltration Over Physical Medium
- T1567: Exfiltration Over Web Service
  - 🟥 T1567.002: Exfiltration to Cloud Storage
  - T1567.001: Exfiltration to Code Repository
- T1029: Scheduled Transfer
- T1537: Transfer Data to Cloud Account

Impact

- T1531: Account Access Removal
- T1485: Data Destruction
- 🟥 T1486: Data Encrypted for Impact
- T1565: Data Manipulation
- T1491: Defacement
- T1561: Disk Wipe
- T1499: Endpoint Denial of Service
- T1495: Firmware Corruption
- 🟥 T1490: Inhibit System Recovery
- T1498: Network Denial of Service
- T1496: Resource Hijacking
- 🟥 T1489: Service Stop
- T1529: System Shutdown/Reboot