Cuba, Software S0625 | MITRE ATT&CK®

Archived: 2026-04-05 15:18:16 UTC

Enterprise T1134 Access Token Manipulation

Cuba has used `SeDebugPrivilege` and `AdjustTokenPrivileges` to elevate privileges.[1]

Enterprise T1059 .001 Command and Scripting Interpreter: PowerShell

Cuba has been dropped onto systems and used for lateral movement via obfuscated PowerShell scripts.[1]

.003 Command and Scripting Interpreter: Windows Command Shell

Cuba has used `cmd.exe /c` and batch files for execution.[1]

Enterprise T1543 .003 Create or Modify System Process: Windows Service

Cuba can modify services by using the `OpenService` and `ChangeServiceConfig` functions.[1]

Enterprise T1486 Data Encrypted for Impact

Cuba has the ability to encrypt system data and add the ".cuba" extension to encrypted files.[1]

Enterprise T1083 File and Directory Discovery

Cuba can enumerate files by using a variety of functions.[1]

Enterprise T1564 .003 Hide Artifacts: Hidden Window

Cuba has executed hidden PowerShell windows.[1]

Enterprise T1070 .004 Indicator Removal: File Deletion

Cuba can use the command `cmd.exe /c del` to delete its artifacts from the system.[1]

Enterprise T1105 Ingress Tool Transfer

Cuba can download files from its C2 server.[1]

Enterprise T1056 .001 Input Capture: Keylogging

Cuba logs keystrokes via polling by using `GetKeyState` and `VkKeyScan` functions.[1]

Enterprise T1680 Local Storage Discovery

Cuba can enumerate local drives, disk type, and disk free space.[1]

Enterprise T1036 .005 Masquerading: Match Legitimate Resource Name or Location

Cuba has been disguised as legitimate 360 Total Security Antivirus and OpenVPN programs.[1]

Enterprise T1106 Native API

Cuba has used several built-in API functions for discovery like GetIpNetTable and NetShareEnum.[1]

Enterprise T1135 Network Share Discovery

Cuba can discover shared resources using the `NetShareEnum` API call.[1]

Enterprise T1027 Obfuscated Files or Information

Cuba has used multiple layers of obfuscation to avoid analysis, including its Base64 encoded payload.[1]

.002 Software Packing

Cuba has a packed payload when delivered.[1]

Enterprise T1057 Process Discovery

Cuba can enumerate processes running on a victim's machine.[1]

Enterprise T1620 Reflective Code Loading

Cuba loaded the payload into memory using PowerShell.[1]

Enterprise T1489 Service Stop

Cuba has a hardcoded list of services and processes to terminate.[1]

Enterprise T1614 .001 System Location Discovery: System Language Discovery

Cuba can check if Russian language is installed on the infected machine by using the function `GetKeyboardLayoutList`.[1]

Enterprise T1016 System Network Configuration Discovery

Cuba can retrieve the ARP cache from the local system by using `GetIpNetTable`.[1]

Enterprise T1049 System Network Connections Discovery

Cuba can use the function `GetIpNetTable` to recover the last connections to the victim's machine.[1]

Enterprise T1007 System Service Discovery

Cuba can query service status using `QueryServiceStatusEx` function.[1]

Source: https://attack.mitre.org/software/S0625