# Flagpro, Software S0696 | MITRE ATT&CK®

Archived: 2026-04-05 12:55:35 UTC

Enterprise T1071 .001 Application Layer Protocol: Web Protocols

Flagpro can communicate with its C2 using HTTP.[1]

Enterprise T1010 Application Window Discovery

Flagpro can check the name of the window displayed on the system.[1]

Enterprise T1547 .001 Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder

Flagpro has dropped an executable file to the startup directory.[1]

Enterprise T1059 .003 Command and Scripting Interpreter: Windows Command Shell

Flagpro can use `cmd.exe` to execute commands received from C2.[1]

.005 Command and Scripting Interpreter: Visual Basic

Flagpro can execute malicious VBA macros embedded in .xlsm files.[1]

Enterprise T1132 .001 Data Encoding: Standard Encoding

Flagpro has encoded bidirectional data communications between a target system and C2 server using Base64.[1]

Enterprise T1005 Data from Local System

Flagpro can collect data from a compromised host, including Windows authentication information.[1]

Enterprise T1041 Exfiltration Over C2 Channel

Flagpro has exfiltrated data to the C2 server.[1]

Enterprise T1070 Indicator Removal

Flagpro can close specific Windows Security and Internet Explorer dialog boxes to mask external connections.[1]

Enterprise T1105 Ingress Tool Transfer

Flagpro can download additional malware from the C2 server.[1]

Enterprise T1036 Masquerading

Flagpro can download malicious files with a .tmp extension and append them with .exe prior to execution.[1]

Enterprise T1106 Native API

Flagpro can use Native API to enable obfuscation including `GetLastError` and `GetTickCount`.[1]

Enterprise T1135 Network Share Discovery

Flagpro has been used to execute `net view` to discover mapped network shares.[1]

Enterprise T1027 Obfuscated Files or Information

Flagpro has been delivered within ZIP or RAR password-protected archived files.[1]

Enterprise T1069 .001 Permission Groups Discovery: Local Groups

Flagpro has been used to execute the `net localgroup administrators` command on a targeted system.[1]

Enterprise T1566 .001 Phishing: Spearphishing Attachment

Flagpro has been distributed via spearphishing as an email attachment.[1]

Enterprise T1057 Process Discovery

Flagpro has been used to run the `tasklist` command on a compromised system.[1]

Enterprise T1018 Remote System Discovery

Flagpro has been used to execute `net view` on a targeted system.[1]

Enterprise T1029 Scheduled Transfer

Flagpro has the ability to wait for a specified time interval between communicating with and executing commands from C2.[1]

Enterprise T1614 .001 System Location Discovery: System Language Discovery

Flagpro can check whether the target system is using Japanese, Taiwanese, or English through detection of specific Windows Security and Internet Explorer dialog.[1]

Enterprise T1016 System Network Configuration Discovery

Flagpro has been used to execute the `ipconfig /all` command on a victim system.[1]

Enterprise T1049 System Network Connections Discovery

Flagpro has been used to execute `netstat -ano` on a compromised host.[1]

Enterprise T1033 System Owner/User Discovery

Flagpro has been used to run the `whoami` command on the system.[1]

Enterprise T1204 .002 User Execution: Malicious File

Flagpro has relied on users clicking a malicious attachment delivered through spearphishing.[1]

---