# FELIXROOT, Software S0267 | MITRE ATT&CK®

Archived: 2026-04-02 12:38:30 UTC

Enterprise T1071 .001 Application Layer Protocol: Web Protocols

FELIXROOT uses HTTP and HTTPS to communicate with the C2 server.[1][2]

Enterprise T1560 Archive Collected Data

FELIXROOT encrypts collected data with AES and Base64 and then sends it to the C2 server.[1]

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

FELIXROOT adds a shortcut file to the startup folder for persistence.[2]

.009 Boot or Logon Autostart Execution: Shortcut Modification

FELIXROOT creates a .LNK file for persistence.[2]

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

FELIXROOT executes batch scripts on the victim's machine, and can launch a reverse shell for command execution.[1][2]

Enterprise T1070 .004 Indicator Removal: File Deletion

FELIXROOT deletes the .LNK file from the startup directory as well as the dropper components.[1]

Enterprise T1105 Ingress Tool Transfer

FELIXROOT downloads and uploads files to and from the victim's machine.[1][2]

Enterprise T1680 Local Storage Discovery

FELIXROOT collects the victim's volume serial number.[1][2]

Enterprise T1112 Modify Registry

FELIXROOT deletes the Registry key `HKCU\Software\Classes\Applications\rundll32.exe\shell\open`.[1]

Enterprise T1027 .013 Obfuscated Files or Information: Encrypted/Encoded File

FELIXROOT encrypts strings in the backdoor using a custom XOR algorithm.[1][2]

Enterprise T1057 Process Discovery

FELIXROOT collects a list of running processes.[2]

Enterprise T1012 Query Registry

FELIXROOT queries the Registry for specific keys for potential privilege escalation and proxy information. FELIXROOT has also used WMI to query the Windows Registry.[1][2]

Enterprise T1518 .001 Software Discovery: Security Software Discovery

FELIXROOT checks for installed security software like antivirus and firewall.[2]

Enterprise T1218 .011 System Binary Proxy Execution: Rundll32

FELIXROOT uses Rundll32 for executing the dropper program.[1][2]

Enterprise T1082 System Information Discovery

FELIXROOT collects the victim’s computer name, processor architecture, OS version, and system type.[1][2]

Enterprise T1016 System Network Configuration Discovery

FELIXROOT collects information about the network including the IP address and DHCP server.[2]

Enterprise T1033 System Owner/User Discovery

FELIXROOT collects the username from the victim’s machine.[1][2]

Enterprise T1124 System Time Discovery

FELIXROOT gathers the time zone information from the victim’s machine.[2]

Enterprise T1047 Windows Management Instrumentation

FELIXROOT uses WMI to query the Windows Registry.[2]

---