MarkiRAT, Software S0652 | MITRE ATT&CK®

Archived: 2026-04-05 14:07:17 UTC

Enterprise T1071 .001 Application Layer Protocol: Web Protocols

MarkiRAT can initiate communication over HTTP/HTTPS for its C2 server.[1]

Enterprise T1197 BITS Jobs

MarkiRAT can use BITS Utility to connect with the C2 server.[1]

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

MarkiRAT can drop its payload into the Startup directory to ensure it automatically runs when the compromised system is started.[1]

.009 Boot or Logon Autostart Execution: Shortcut Modification

MarkiRAT can modify the shortcut that launches Telegram by replacing its path with the malicious payload to launch with the legitimate executable.[1]

Enterprise T1115 Clipboard Data

MarkiRAT can capture clipboard content.[1]

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

MarkiRAT can utilize cmd.exe to execute commands in a victim's environment.[1]

Enterprise T1555 .005 Credentials from Password Stores: Password Managers

MarkiRAT can gather information from the Keepass password manager.[1]

Enterprise T1005 Data from Local System

MarkiRAT can upload data from the victim's machine to the C2 server.[1]

Enterprise T1074 .001 Data Staged: Local Data Staging

MarkiRAT can store collected data locally in a created .nfo file.[1]

Enterprise T1041 Exfiltration Over C2 Channel

MarkiRAT can exfiltrate locally stored data via its C2.[1]

Enterprise T1083 File and Directory Discovery

MarkiRAT can look for files carrying specific extensions such as: .rtf, .doc, .docx, .xls, .xlsx, .ppt, .pptx, .pps, .ppsx, .txt, .gpg, .pkr, .kdbx, .key, and .jpb.[1]

Enterprise T1105 Ingress Tool Transfer

MarkiRAT can download additional files and tools from its C2 server, including through the use of BITSAdmin.[1]

Enterprise T1056 .001 Input Capture: Keylogging

MarkiRAT can capture all keystrokes on a compromised host.[1]

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

MarkiRAT can masquerade as `update.exe` and `svehost.exe`; it has also mimicked legitimate Telegram and Chrome files.[1]

Enterprise T1106 Native API

MarkiRAT can run the ShellExecuteW API via the Windows Command Shell.[1]

Enterprise T1057 Process Discovery

MarkiRAT can search for different processes on a system.[1]

Enterprise T1113 Screen Capture

MarkiRAT can capture screenshots that are initially saved as ‘scr.jpg’.[1]

Enterprise T1518 Software Discovery

MarkiRAT can check for the Telegram installation directory by enumerating the files on disk.[1]

.001 Security Software Discovery

MarkiRAT can check for running processes on the victim’s machine to look for Kaspersky and Bitdefender antivirus products.[1]

Enterprise T1082 System Information Discovery

MarkiRAT can obtain the computer name from a compromised host.[1]

Enterprise T1614 .001 System Location Discovery: System Language Discovery

MarkiRAT can use the `GetKeyboardLayout` API to check if a compromised host's keyboard is set to Persian.[1]

Enterprise T1033 System Owner/User Discovery

MarkiRAT can retrieve the victim’s username.[1]

Source: https://attack.mitre.org/software/S0652