Micropsia, Software S0339 | MITRE ATT&CK®

Archived: 2026-04-05 15:06:44 UTC

Enterprise T1071 .001 Application Layer Protocol: Web Protocols

Micropsia uses HTTP and HTTPS for C2 network communications.[1][2]

Enterprise T1560 .001 Archive Collected Data: Archive via Utility

Micropsia creates a RAR archive based on collected files on the victim's machine.[2]

Enterprise T1123 Audio Capture

Micropsia can perform microphone recording.[2]

Enterprise T1119 Automated Collection

Micropsia executes an RAR tool to recursively archive files based on a predefined list of file extensions (*.xls*, .xlsx, *.csv*, .odt, *.doc*, .docx, *.ppt*, .pptx, *.pdf*, .mdb, *.accdb*, .accde, *.txt).[2]

Enterprise T1547 .009 Boot or Logon Autostart Execution: Shortcut Modification

Micropsia creates a shortcut to maintain persistence.[1]

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

Micropsia creates a command-line shell using cmd.exe.[2]

Enterprise T1083 File and Directory Discovery

Micropsia can perform a recursive directory listing for all volume drives available on the victim's machine and can also fetch specific files by their paths.[2]

Enterprise T1564 .001 Hide Artifacts: Hidden Files and Directories

Micropsia creates a new hidden directory to store all components' outputs in a dedicated sub-folder for each.[2]

Enterprise T1105 Ingress Tool Transfer

Micropsia can download and execute an executable from the C2 server.[1][2]

Enterprise T1056 .001 Input Capture: Keylogging

Micropsia has keylogging capabilities.[2]

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

Micropsia obfuscates the configuration with a custom Base64 and XOR.[1][2]

Enterprise T1113 Screen Capture

Micropsia takes screenshots every 90 seconds by calling the Gdi32.BitBlt API.[2]

Enterprise T1518 .001 Software Discovery: Security Software Discovery

Micropsia searches for anti-virus software and firewall products installed on the victim's machine using WMI.[1] [2]

Enterprise T1082 System Information Discovery

Micropsia gathers the hostname and OS version from the victim's machine.[1][2]

Enterprise T1033 System Owner/User Discovery

Micropsia collects the username from the victim's machine.[1]

Enterprise T1047 Windows Management Instrumentation

Micropsia searches for anti-virus software and firewall products installed on the victim's machine using WMI.[1] [2]
