jRAT, Software S0283 | MITRE ATT&CK®

Archived: 2026-04-02 11:13:27 UTC

Enterprise T1123 Audio Capture

jRAT can capture microphone recordings.[1]

Enterprise T1037 .005 Boot or Logon Initialization Scripts: Startup Items

jRAT can list and manage startup entries.[1]

Enterprise T1115 Clipboard Data

jRAT can capture clipboard data.[1]

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

jRAT has command line access.[1]

.005 Command and Scripting Interpreter: Visual Basic

jRAT has been distributed as HTA files with VBScript.[1]

.007 Command and Scripting Interpreter: JavaScript

jRAT has been distributed as HTA files with JScript.[1]

Enterprise T1555 .003 Credentials from Password Stores: Credentials from Web Browsers

jRAT can capture passwords from common web browsers such as Internet Explorer, Google Chrome, and Firefox.[1]

Enterprise T1083 File and Directory Discovery

jRAT can browse file systems.[1][4]

Enterprise T1070 .004 Indicator Removal: File Deletion

jRAT has a function to delete files from the victim’s machine.[2]

Enterprise T1105 Ingress Tool Transfer

jRAT can download and execute files.[2][1][4]

Enterprise T1056 .001 Input Capture: Keylogging

jRAT has the capability to log keystrokes from the victim's machine, both offline and online.[2][1]

Enterprise T1027 Obfuscated Files or Information

jRAT's Java payload is encrypted with AES.[2] Additionally, backdoor files are encrypted using DES as a stream cipher. Later variants of jRAT also incorporated AV evasion methods such as Java bytecode obfuscation via the commercial Allatori obfuscation tool.[4]

.002 Software Packing

jRAT payloads have been packed.[1]

Enterprise T1120 Peripheral Device Discovery

jRAT can map UPnP ports.[1]

Enterprise T1057 Process Discovery

jRAT can query and kill system processes.[4]

Enterprise T1090 Proxy

jRAT can serve as a SOCKS proxy server.[1]

Enterprise T1021 .001 Remote Services: Remote Desktop Protocol

jRAT can support RDP control.[1]

Enterprise T1029 Scheduled Transfer

jRAT can be configured to reconnect at certain intervals.[1]

Enterprise T1113 Screen Capture

jRAT has the capability to take screenshots of the victim's machine.[2][1]

Enterprise T1518 .001 Software Discovery: Security Software Discovery

jRAT can list security software, such as by using WMIC to identify anti-virus products installed on the victim's machine and to obtain firewall details.[2][1]

Enterprise T1082 System Information Discovery

jRAT collects information about the OS (version, build type, install date) as well as system up-time upon receiving a connection from a backdoor.[4]

Enterprise T1016 System Network Configuration Discovery

jRAT can gather victim internal and external IPs.[1]

Enterprise T1049 System Network Connections Discovery

jRAT can list network connections.[1]

Enterprise T1007 System Service Discovery

jRAT can list local services.[1]

Enterprise T1552 .001 Unsecured Credentials: Credentials In Files

jRAT can capture passwords from common chat applications such as MSN Messenger, AOL, Instant Messenger, and and Google Talk.[1]

.004 Unsecured Credentials: Private Keys

jRAT can steal keys for VPNs and cryptocurrency wallets.[1]

Enterprise T1125 Video Capture

jRAT has the capability to capture video from a webcam.[2][1]

Enterprise T1047 Windows Management Instrumentation

jRAT uses WMIC to identify anti-virus products installed on the victim’s machine and to obtain firewall details.[2]
