Kazuar, Software S0265 | MITRE ATT&CK®

Archived: 2026-04-05 14:38:32 UTC

Enterprise T1087 .001 Account Discovery: Local Account

Kazuar gathers information on local groups and members on the victim's machine.[1]

Enterprise T1071 .001 Application Layer Protocol: Web Protocols

Kazuar uses HTTP and HTTPS to communicate with the C2 server. Kazuar can also act as a webserver and listen for inbound HTTP requests through an exposed API.[1]

.002 Application Layer Protocol: File Transfer Protocols

Kazuar uses FTP and FTPS to communicate with the C2 server.[1]

Enterprise T1010 Application Window Discovery

Kazuar gathers information about opened windows.[1]

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

Kazuar adds a sub-key under several Registry run keys.[1]

.009 Boot or Logon Autostart Execution: Shortcut Modification

Kazuar adds a .lnk file to the Windows startup folder.[1]

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

Kazuar uses cmd.exe to execute commands on the victim's machine.[1]

.004 Command and Scripting Interpreter: Unix Shell

Kazuar uses /bin/bash to execute commands on the victim's machine.[1]

Enterprise T1543 .003 Create or Modify System Process: Windows Service

Kazuar can install itself as a new service.[1]

Enterprise T1485 Data Destruction

Kazuar can overwrite files with random data before deleting them.[1]

Enterprise T1132 .001 Data Encoding: Standard Encoding

Kazuar encodes communications to the C2 server in Base64.[1]

Enterprise T1005 Data from Local System

Kazuar uploads files from a specified directory to the C2 server.[1]

Enterprise T1074 .001 Data Staged: Local Data Staging

Kazuar stages command output and collected data in files before exfiltration.[1]

Enterprise T1008 Fallback Channels

Kazuar can accept multiple URLs for C2 servers.[1]

Enterprise T1083 File and Directory Discovery

Kazuar finds a specified directory, lists the files and metadata about those files.[1]

Enterprise T1070 .004 Indicator Removal: File Deletion

Kazuar can delete files.[1]

Enterprise T1105 Ingress Tool Transfer

Kazuar downloads additional plug-ins to load on the victim’s machine, including the ability to upgrade and replace its own binary.[1]

Enterprise T1680 Local Storage Discovery

Kazuar gathers information on local drives.[1]

Enterprise T1027 Obfuscated Files or Information

Kazuar is obfuscated using the open source ConfuserEx protector. Kazuar also obfuscates the name of created files/folders/mutexes and encrypts debug messages written to log files using the Rijndael cipher.[1]

Enterprise T1069 .001 Permission Groups Discovery: Local Groups

Kazuar gathers information about local groups and members.[1]

Enterprise T1057 Process Discovery

Kazuar obtains a list of running processes through WMI querying and the `ps` command.[1]

Enterprise T1055 .001 Process Injection: Dynamic-link Library Injection

If running in a Windows environment, Kazuar saves a DLL to disk that is injected into the explorer.exe process to execute the payload. Kazuar can also be configured to inject and execute within specific processes.[1]

Enterprise T1090 .001 Proxy: Internal Proxy

Kazuar has used internal nodes on the compromised network for C2 communications.[2]

Enterprise T1029 Scheduled Transfer

Kazuar can sleep for a specific time and be set to communicate at specific intervals.[1]

Enterprise T1113 Screen Capture

Kazuar captures screenshots of the victim's screen.[1]

Enterprise T1082 System Information Discovery

Kazuar gathers information on the system.[1]

Enterprise T1016 System Network Configuration Discovery

Kazuar gathers information about network adapters.[1]

Enterprise T1033 System Owner/User Discovery

Kazuar gathers information on users.[1]

Enterprise T1125 Video Capture

Kazuar captures images from the webcam.[1]

Enterprise T1102 .002 Web Service: Bidirectional Communication

Kazuar has used compromised WordPress blogs as C2 servers.[1]

Enterprise T1047 Windows Management Instrumentation

Kazuar obtains a list of running processes through WMI querying.[1]
