TajMahal, Software S0467 | MITRE ATT&CK®

Archived: 2026-04-05 17:20:34 UTC

Enterprise T1560 .002 Archive Collected Data: Archive via Library

TajMahal has the ability to use the open source libraries XZip/Xunzip and zlib to compress files.[1]

Enterprise T1123 Audio Capture

TajMahal has the ability to capture VoiceIP application audio on an infected host.[1]

Enterprise T1119 Automated Collection

TajMahal has the ability to index and compress files into a send queue for exfiltration.[1]

Enterprise T1020 Automated Exfiltration

TajMahal has the ability to manage an automated queue of egress files and commands sent to its C2.[1]

Enterprise T1115 Clipboard Data

TajMahal has the ability to steal data from the clipboard of an infected host.[1]

Enterprise T1005 Data from Local System

TajMahal has the ability to steal documents from the local system including the print spooler queue.[1]

Enterprise T1025 Data from Removable Media

TajMahal has the ability to steal written CD images and files of interest from previously connected removable drives when they become available again.[1]

Enterprise T1041 Exfiltration Over C2 Channel

TajMahal has the ability to send collected files over its C2.[1]

Enterprise T1083 File and Directory Discovery

TajMahal has the ability to index files from drives, user profiles, and removable drives.[1]

Enterprise T1056 .001 Input Capture: Keylogging

TajMahal has the ability to capture keystrokes on an infected host.[1]

Enterprise T1112 Modify Registry

TajMahal can set the `KeepPrintedJobs` attribute for configured printers in `SOFTWARE\Microsoft\Windows NT\CurrentVersion\Print\Printers` to enable document stealing.[1]

Enterprise T1027 Obfuscated Files or Information

TajMahal has used an encrypted Virtual File System to store plugins.[1]

Enterprise T1120 Peripheral Device Discovery

TajMahal has the ability to identify connected Apple devices.[1]

Enterprise T1057 Process Discovery

TajMahal has the ability to identify running processes and associated plugins on an infected host.[1]

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

TajMahal has the ability to inject DLLs for malicious plugins into running processes.[1]

Enterprise T1113 Screen Capture

TajMahal has the ability to take screenshots on an infected host including capturing content from windows of instant messaging applications.[1]

Enterprise T1129 Shared Modules

TajMahal has the ability to inject the `LoadLibrary` call template DLL into running processes.[1]

Enterprise T1518 Software Discovery

TajMahal has the ability to identify the Internet Explorer (IE) version on an infected host.[1]

.001 Security Software Discovery

TajMahal has the ability to identify which anti-virus products, firewalls, and anti-spyware products are in use.[1]

Enterprise T1539 Steal Web Session Cookie

TajMahal has the ability to steal web session cookies from Internet Explorer, Netscape Navigator, FireFox and RealNetworks applications.[1]

Enterprise T1082 System Information Discovery

TajMahal has the ability to identify hardware information, the computer name, and OS information on an infected host.[1]

Enterprise T1016 System Network Configuration Discovery

TajMahal has the ability to identify the MAC address on an infected host.[1]

Enterprise T1124 System Time Discovery

TajMahal has the ability to determine local time on a compromised host.[1]

Enterprise T1125 Video Capture

TajMahal has the ability to capture webcam video.[1]

Source: https://attack.mitre.org/software/S0467