Attor, Software S0438 | MITRE ATT&CK®

Archived: 2026-04-05 14:43:34 UTC

Enterprise T1071 .002 Application Layer Protocol: File Transfer Protocols

Attor has used FTP protocol for C2 communication.[1]

Enterprise T1010 Application Window Discovery

Attor can obtain application window titles and then determines which windows to perform Screen Capture on.[1]

Enterprise T1560 .003 Archive Collected Data: Archive via Custom Method

Attor encrypts collected data with a custom implementation of Blowfish and RSA ciphers.[1]

Enterprise T1123 Audio Capture

Attor's has a plugin that is capable of recording audio using available input sound devices.[1]

Enterprise T1119 Automated Collection

Attor has automatically collected data about the compromised system.[1]

Enterprise T1020 Automated Exfiltration

Attor has a file uploader plugin that automatically exfiltrates the collected data and log files to the C2 server.[1]

Enterprise T1037 .001 Boot or Logon Initialization Scripts: Logon Script (Windows)

Attor's dispatcher can establish persistence via adding a Registry key with a logon script `HKEY_CURRENT_USER\Environment "UserInitMprLogonScript"` .[1]

Enterprise T1115 Clipboard Data

Attor has a plugin that collects data stored in the Windows clipboard by using the OpenClipboard and GetClipboardData APIs.[1]

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

Attor's dispatcher can establish persistence by registering a new service.[1]

Enterprise T1074 .001 Data Staged: Local Data Staging

Attor has staged collected data in a central upload directory prior to exfiltration.[1]

Enterprise T1573 .001 Encrypted Channel: Symmetric Cryptography

Attor has encrypted data symmetrically using a randomly generated Blowfish (OFB) key which is encrypted with a public RSA key.[1]

.002 Encrypted Channel: Asymmetric Cryptography

Attor's Blowfish key is encrypted with a public RSA key.[1]

Enterprise T1041 Exfiltration Over C2 Channel

Attor has exfiltrated data over the C2 channel.[1]

Enterprise T1083 File and Directory Discovery

Attor has a plugin that enumerates files with specific extensions on all hard disk drives and stores file information in encrypted log files.[1]

Enterprise T1564 .001 Hide Artifacts: Hidden Files and Directories

Attor can set attributes of log files and directories to HIDDEN, SYSTEM, ARCHIVE, or a combination of those. [1]

Enterprise T1070 .004 Indicator Removal: File Deletion

Attor's plugin deletes the collected files and log files after exfiltration.[1]

.006 Indicator Removal: Timestomp

Attor has manipulated the time of last access to files and registry keys after they have been created or modified.[1]

Enterprise T1105 Ingress Tool Transfer

Attor can download additional plugins, updates and other files. [1]

Enterprise T1056 .001 Input Capture: Keylogging

One of Attor's plugins can collect user credentials via capturing keystrokes and can capture keystrokes pressed within the window of the injected process.[1]

Enterprise T1680 Local Storage Discovery

Attor monitors the free disk space on the system.[1]

Enterprise T1036 .004 Masquerading: Masquerade Task or Service

Attor's dispatcher disguises itself as a legitimate task (i.e., the task name and description appear legitimate).[1]

Enterprise T1112 Modify Registry

Attor's dispatcher can modify the Run registry key.[1]

Enterprise T1106 Native API

Attor's dispatcher has used CreateProcessW API for execution.[1]

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

Strings in Attor's components are encrypted with a XOR cipher, using a hardcoded key and the configuration data, log files and plugins are encrypted using a hybrid encryption scheme of Blowfish-OFB combined with RSA.[1]

Enterprise T1120 Peripheral Device Discovery

Attor has a plugin that collects information about inserted storage devices, modems, and phone devices.[1]

Enterprise T1055 Process Injection

Attor's dispatcher can inject itself into running processes to gain higher privileges and to evade detection.[1]

.004 Asynchronous Procedure Call

Attor performs the injection by attaching its code into the APC queue using NtQueueApcThread API.[1]

Enterprise T1090 .003 Proxy: Multi-hop Proxy

Attor has used Tor for C2 communication.[1]

Enterprise T1012 Query Registry

Attor has opened the registry and performed query searches.[1]

Enterprise T1053 .005 Scheduled Task/Job: Scheduled Task

Attor's installer plugin can schedule a new task that loads the dispatcher on boot/logon.[1]

Enterprise T1113 Screen Capture

Attor's has a plugin that captures screenshots of the target applications.[1]

Enterprise T1129 Shared Modules

Attor's dispatcher can execute additional plugins by loading the respective DLLs.[1]

Enterprise T1218 .011 System Binary Proxy Execution: Rundll32

Attor's installer plugin can schedule rundll32.exe to load the dispatcher.[1]

Enterprise T1569 .002 System Services: Service Execution

Attor's dispatcher can be executed as a service.[1]

Enterprise T1497 .001 Virtualization/Sandbox Evasion: System Checks

Attor can detect whether it is executed in some virtualized or emulated environment by searching for specific artifacts, such as communication with I/O ports and using VM-specific instructions.[1]
