InvisiMole, Software S0260 | MITRE ATT&CK®

Archived: 2026-04-05 14:45:13 UTC

Enterprise T1548 .002 Abuse Elevation Control Mechanism: Bypass User Account Control

InvisiMole can use fileless UAC bypass and create an elevated COM object to escalate privileges.[1][2]

Enterprise T1087 .001 Account Discovery: Local Account

InvisiMole has a command to list account information on the victim's machine.[1]

Enterprise T1071 .001 Application Layer Protocol: Web Protocols

InvisiMole uses HTTP for C2 communications.[1]

.004 Application Layer Protocol: DNS

InvisiMole has used a custom implementation of DNS tunneling to embed C2 communications in DNS requests and replies.[2]

Enterprise T1010 Application Window Discovery

InvisiMole can enumerate windows and child windows on a compromised host.[1][2]

Enterprise T1560 .001 Archive Collected Data: Archive via Utility

InvisiMole uses WinRAR to compress data that is intended to be exfiltrated.[1]

.002 Archive Collected Data: Archive via Library

InvisiMole can use zlib to compress and decompress data.[1][2]

.003 Archive Collected Data: Archive via Custom Method

InvisiMole uses a variation of the XOR cipher to encrypt files before exfiltration.[1]

Enterprise T1123 Audio Capture

InvisiMole can record sound using input audio devices.[1][2]

Enterprise T1119 Automated Collection

InvisiMole can sort and collect specific documents as well as generate a list of all files on a newly inserted drive and store them in an encrypted file.[1][2]

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

InvisiMole can place a lnk file in the Startup Folder to achieve persistence.[2]

.009 Boot or Logon Autostart Execution: Shortcut Modification

InvisiMole can use a .lnk shortcut for the Control Panel to establish persistence.[2]

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

InvisiMole can launch a remote shell to execute commands.[1][2]

.007 Command and Scripting Interpreter: JavaScript

InvisiMole can use a JavaScript file as part of its execution chain.[2]

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

InvisiMole can register a Windows service named CsPower as part of its execution chain, and a Windows service named clr_optimization_v2.0.51527_X86 to achieve persistence.[2]

Enterprise T1132 .002 Data Encoding: Non-Standard Encoding

InvisiMole can use a modified base32 encoding to encode data within the subdomain of C2 requests.[2]

Enterprise T1005 Data from Local System

InvisiMole can collect data from the system, and can monitor changes in specified directories.[1]

Enterprise T1025 Data from Removable Media

InvisiMole can collect jpeg files from connected MTP devices.[2]

Enterprise T1001 .003 Data Obfuscation: Protocol or Service Impersonation

InvisiMole can mimic HTTP protocol with custom HTTP "verbs" HIDE, ZVVP, and NOP.[1][2]

Enterprise T1074 .001 Data Staged: Local Data Staging

InvisiMole determines a working directory where it stores all the gathered data about the compromised machine.[1][2]

Enterprise T1140 Deobfuscate/Decode Files or Information

InvisiMole can decrypt, unpack and load a DLL from its resources, or from blobs encrypted with Data Protection API, two-key triple DES, and variations of the XOR cipher.[1][2]

Enterprise T1573 .001 Encrypted Channel: Symmetric Cryptography

InvisiMole uses variations of a simple XOR encryption routine for C&C communications.[1]

Enterprise T1480 .001 Execution Guardrails: Environmental Keying

InvisiMole can use Data Protection API to encrypt its components on the victim's computer, to evade detection, and to make sure the payload can only be decrypted and loaded on one specific compromised computer.[2]

Enterprise T1203 Exploitation for Client Execution

InvisiMole has installed legitimate but vulnerable Total Video Player software and wdigest.dll library drivers on compromised hosts to exploit stack overflow and input validation vulnerabilities for code execution.[2]

Enterprise T1068 Exploitation for Privilege Escalation

InvisiMole has exploited CVE-2007-5633 vulnerability in the speedfan.sys driver to obtain kernel mode privileges.[2]

Enterprise T1210 Exploitation of Remote Services

InvisiMole can spread within a network via the BlueKeep (CVE-2019-0708) and EternalBlue (CVE-2017-0144) vulnerabilities in RDP and SMB respectively.[2]

Enterprise T1008 Fallback Channels

InvisiMole has been configured with several servers available for alternate C2 communications.[1][2]

Enterprise T1083 File and Directory Discovery

InvisiMole can list information about files in a directory and recently opened or used documents. InvisiMole can also search for specific files by supplied file mask.[1]

Enterprise T1564 .001 Hide Artifacts: Hidden Files and Directories

InvisiMole can create hidden system directories.[2]

.003 Hide Artifacts: Hidden Window

InvisiMole has executed legitimate tools in hidden windows.[2]

Enterprise T1574 .001 Hijack Execution Flow: DLL

InvisiMole can be launched by using DLL search order hijacking in which the wrapper DLL is placed in the same folder as explorer.exe and loaded during startup into the Windows Explorer process instead of the legitimate library.[1]

Enterprise T1562 .004 Impair Defenses: Disable or Modify System Firewall

InvisiMole has a command to disable routing and the Firewall on the victim's machine.[1]

Enterprise T1070 .004 Indicator Removal: File Deletion

InvisiMole has deleted files and directories including XML and files successfully uploaded to C2 servers.[1][2]

.005 Indicator Removal: Network Share Connection Removal

InvisiMole can disconnect previously connected remote drives.[1]

.006 Indicator Removal: Timestomp

InvisiMole samples were timestomped by the authors by setting the PE timestamps to all zero values. InvisiMole also has a built-in command to modify file times.[1]

Enterprise T1105 Ingress Tool Transfer

InvisiMole can upload files to the victim's machine for operations.[1][2]

Enterprise T1490 Inhibit System Recovery

InvisiMole can can remove all system restore points.[1]

Enterprise T1056 .001 Input Capture: Keylogging

InvisiMole can capture keystrokes on a compromised host.[2]

Enterprise T1559 .001 Inter-Process Communication: Component Object Model

InvisiMole can use the `ITaskService`, `ITaskDefinition` and `ITaskSettings` COM interfaces to schedule a task.[2]

Enterprise T1680 Local Storage Discovery

InvisiMole can gather information on the mapped drives and system volume serial number.[1][2]

Enterprise T1036 .004 Masquerading: Masquerade Task or Service

InvisiMole has attempted to disguise itself by registering under a seemingly legitimate service name.[2]

.005 Masquerading: Match Legitimate Resource Name or Location

InvisiMole has disguised its droppers as legitimate software or documents, matching their original names and locations, and saved its files as mpr.dll in the Windows folder.[1][2]

Enterprise T1112 Modify Registry

InvisiMole has a command to create, set, copy, or delete a specified Registry key or value.[1][2]

Enterprise T1106 Native API

InvisiMole can use winapiexec tool for indirect execution of `ShellExecuteW` and `CreateProcessA`.[2]

Enterprise T1046 Network Service Discovery

InvisiMole can scan the network for open ports and vulnerable instances of RDP and SMB protocols.[2]

Enterprise T1135 Network Share Discovery

InvisiMole can gather network share information.[1]

Enterprise T1095 Non-Application Layer Protocol

InvisiMole has used TCP to download additional modules.[2]

Enterprise T1027 Obfuscated Files or Information

InvisiMole avoids analysis by encrypting all strings, internal files, configuration data and by using a custom executable format.[1][2]

.005 Indicator Removal from Tools

InvisiMole has undergone regular technical improvements in an attempt to evade detection.[2]

Enterprise T1057 Process Discovery

InvisiMole can obtain a list of running processes.[1][2]

Enterprise T1055 Process Injection

InvisiMole can inject itself into another process to avoid detection including use of a technique called ListPlanting that customizes the sorting algorithm in a ListView structure.[2]

.002 Portable Executable Injection

InvisiMole can inject its backdoor as a portable executable into a target process.[2]

.004 Asynchronous Procedure Call

InvisiMole can inject its code into a trusted process via the APC queue.[2]

.015 ListPlanting

InvisiMole has used ListPlanting to inject code into a trusted process.[2]

Enterprise T1090 .001 Proxy: Internal Proxy

InvisiMole can function as a proxy to create a server that relays communication between the client and C&C server, or between two clients.[1]

.002 Proxy: External Proxy

InvisiMole InvisiMole can identify proxy servers used by the victim and use them for C2 communication.[1][2]

Enterprise T1012 Query Registry

InvisiMole can enumerate Registry values, keys, and data.[1]

Enterprise T1053 .005 Scheduled Task/Job: Scheduled Task

InvisiMole has used scheduled tasks named `MSST` and `\Microsoft\Windows\Autochk\Scheduled` to establish persistence.[2]

Enterprise T1113 Screen Capture

InvisiMole can capture screenshots of not only the entire screen, but of each separate window open, in case they are overlapping.[1][2]

Enterprise T1518 Software Discovery

InvisiMole can collect information about installed software used by specific users, software executed on user login, and software executed by each system.[1][2]

.001 Security Software Discovery

InvisiMole can check for the presence of network sniffers, AV, and BitDefender firewall.[2]

Enterprise T1218 .002 System Binary Proxy Execution: Control Panel

InvisiMole can register itself for execution and persistence via the Control Panel.[2]

.011 System Binary Proxy Execution: Rundll32

InvisiMole has used rundll32.exe for execution.[2]

Enterprise T1082 System Information Discovery

InvisiMole can gather information on the OS version, computer name, DEP policy, and memory size.[1][2]

Enterprise T1016 System Network Configuration Discovery

InvisiMole gathers information on the IP forwarding table, MAC address, configured proxy, and network SSID.[1][2]

Enterprise T1033 System Owner/User Discovery

InvisiMole lists local users and session information.[1]

Enterprise T1007 System Service Discovery

InvisiMole can obtain running services on the victim.[1]

Enterprise T1569 .002 System Services: Service Execution

InvisiMole has used Windows services as a way to execute its malicious payload.[2]

Enterprise T1124 System Time Discovery

InvisiMole gathers the local system time from the victim's machine.[1][2]

Enterprise T1080 Taint Shared Content

InvisiMole can replace legitimate software or documents in the compromised network with their trojanized versions, in an attempt to propagate itself within the network.[2]

Enterprise T1204 .002 User Execution: Malicious File

InvisiMole can deliver trojanized versions of software and documents, relying on user execution.[2]

Enterprise T1125 Video Capture

InvisiMole can remotely activate the victim's webcam to capture content.[1][2]

Enterprise T1497 .001 Virtualization/Sandbox Evasion: System Checks

InvisiMole can check for artifacts of VirtualBox, Virtual PC and VMware environment, and terminate itself if they are detected.[2]
