Metamorfo, Software S0455 | MITRE ATT&CK®

Archived: 2026-04-05 18:39:30 UTC

Enterprise T1071 .001 Application Layer Protocol: Web Protocols

Metamorfo has used HTTP for C2.[1][2]

Enterprise T1010 Application Window Discovery

Metamorfo can enumerate all windows on the victim’s machine.[3][4]

Enterprise T1119 Automated Collection

Metamorfo has automatically collected mouse clicks, continuous screenshots on the machine, and set timers to collect the contents of the clipboard and website browsing.[3]

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

Metamorfo has configured persistence to the Registry key `HKCU\Software\Microsoft\Windows\CurrentVersion\Run, Spotify =% APPDATA%\Spotify\Spotify.exe` and used .LNK files in the startup folder to achieve persistence.[1][3][4][2]

Enterprise T1115 Clipboard Data

Metamorfo has a function to hijack data from the clipboard by monitoring the contents of the clipboard and replacing the cryptocurrency wallet with the attacker's.[4][2]

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

Metamorfo has used `cmd.exe /c` to execute files.[1]

.005 Command and Scripting Interpreter: Visual Basic

Metamorfo has used VBS code on victims’ systems.[3]

.007 Command and Scripting Interpreter: JavaScript

Metamorfo includes payloads written in JavaScript.[1]

Enterprise T1565 .002 Data Manipulation: Transmitted Data Manipulation

Metamorfo has a function that can watch the contents of the system clipboard for valid bitcoin addresses, which it then overwrites with the attacker's address.[4][2]

Enterprise T1140 Deobfuscate/Decode Files or Information

Upon execution, Metamorfo has unzipped itself after being downloaded to the system and has performed string decryption.[1][3][2]

Enterprise T1573 .001 Encrypted Channel: Symmetric Cryptography

Metamorfo has encrypted C2 commands with AES-256.[2]

.002 Encrypted Channel: Asymmetric Cryptography

Metamorfo's C2 communication has been encrypted using OpenSSL.[1]

Enterprise T1041 Exfiltration Over C2 Channel

Metamorfo can send the data it collects to the C2 server.[2]

Enterprise T1083 File and Directory Discovery

Metamorfo has searched the Program Files directories for specific folders and has searched for strings related to its mutexes.[1][4][3]

Enterprise T1564 .003 Hide Artifacts: Hidden Window

Metamorfo has hidden its GUI using the ShowWindow() WINAPI call.[1]

Enterprise T1574 .001 Hijack Execution Flow: DLL

Metamorfo has side-loaded its malicious DLL file.[1][3][2]

Enterprise T1562 .001 Impair Defenses: Disable or Modify Tools

Metamorfo has a function to kill processes associated with defenses and can prevent certain processes from launching.[1][3]

Enterprise T1070 Indicator Removal

Metamorfo has a command to delete a Registry key it uses, `\Software\Microsoft\Internet Explorer\notes`.[3]

.004 File Deletion

Metamorfo has deleted itself from the system after execution.[1][4]

Enterprise T1105 Ingress Tool Transfer

Metamorfo has used MSI files to download additional files to execute.[1][3][4][2]

Enterprise T1056 .001 Input Capture: Keylogging

Metamorfo has a command to launch a keylogger and capture keystrokes on the victim’s machine.[4][2]

.002 Input Capture: GUI Input Capture

Metamorfo has displayed fake forms on top of banking sites to intercept credentials from victims.[3]

Enterprise T1036 .005 Masquerading: Match Legitimate Resource Name or Location

Metamorfo has disguised an MSI file as the Adobe Acrobat Reader Installer and has masqueraded payloads as OneDrive, WhatsApp, or Spotify, for example.[1][2]

Enterprise T1112 Modify Registry

Metamorfo has written process names to the Registry, disabled IE browser features, deleted Registry keys, and changed the ExtendedUIHoverTime key.[1][4][3][2]

Enterprise T1106 Native API

Metamorfo has used native WINAPI calls.[1][4]

Enterprise T1095 Non-Application Layer Protocol

Metamorfo has used raw TCP for C2.[3]

Enterprise T1571 Non-Standard Port

Metamorfo has communicated with hosts over raw TCP on port 9999.[3]

Enterprise T1027 .002 Obfuscated Files or Information: Software Packing

Metamorfo has used VMProtect to pack and protect files.[4]

.013 Obfuscated Files or Information: Encrypted/Encoded File

Metamorfo has encrypted payloads and strings.[1][2]

Enterprise T1566 .001 Phishing: Spearphishing Attachment

Metamorfo has been delivered to victims via emails with malicious HTML attachments.[3][2]

Enterprise T1057 Process Discovery

Metamorfo has performed process name checks and has monitored applications.[1]

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

Metamorfo has injected a malicious DLL into the Windows Media Player process (wmplayer.exe).[1]

Enterprise T1113 Screen Capture

Metamorfo can collect screenshots of the victim’s machine.[3][2]

Enterprise T1129 Shared Modules

Metamorfo had used AutoIt to load and execute the DLL payload.[4]

Enterprise T1518 Software Discovery

Metamorfo has searched the compromised system for banking applications.[3][2]

.001 Security Software Discovery

Metamorfo collects a list of installed antivirus software from the victim’s system.[4][2]

Enterprise T1553 .002 Subvert Trust Controls: Code Signing

Metamorfo has digitally signed executables using AVAST Software certificates.[1]

Enterprise T1218 .005 System Binary Proxy Execution: Mshta

Metamorfo has used mshta.exe to execute a HTA payload.[3]

.007 System Binary Proxy Execution: Msiexec

Metamorfo has used MsiExec.exe to automatically execute files.[4][2]

Enterprise T1082 System Information Discovery

Metamorfo has collected the hostname and operating system version from the compromised host.[3][4][2]

Enterprise T1033 System Owner/User Discovery

Metamorfo has collected the username from the victim's machine.[2]

Enterprise T1124 System Time Discovery

Metamorfo uses JavaScript to get the system time.[1]

Enterprise T1204 .002 User Execution: Malicious File

Metamorfo requires the user to double-click the executable to run the malicious HTA file or to download a malicious installer.[3][2]

Enterprise T1497 Virtualization/Sandbox Evasion

Metamorfo has embedded a "vmdetect.exe" executable to identify virtual machines at the beginning of execution.[1]

Enterprise T1102 .001 Web Service: Dead Drop Resolver

Metamorfo has used YouTube to store and hide C&C server domains.[2]

.003 Web Service: One-Way Communication

Metamorfo has downloaded a zip file for execution on the system.[1][3][4]

Source: https://attack.mitre.org/software/S0455