# PipeMon, Software S0501 | MITRE ATT&CK®

Archived: 2026-04-05 14:05:08 UTC

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

PipeMon installer can use UAC bypass techniques to install the payload.[1]

Enterprise T1134 .002 Access Token Manipulation: Create Process with Token

PipeMon can attempt to gain administrative privileges using token impersonation.[1]

.004 Access Token Manipulation: Parent PID Spoofing

PipeMon can use parent PID spoofing to elevate privileges.[1]

Enterprise T1547 .012 Boot or Logon Autostart Execution: Print Processors

The PipeMon installer has modified the Registry key `HKLM\SYSTEM\CurrentControlSet\Control\Print\Environments\Windows x64\Print Processors` to install PipeMon as a Print Processor.[1]

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

PipeMon can establish persistence by registering a malicious DLL as an alternative Print Processor which is loaded when the print spooler service starts.[1]

Enterprise T1140 Deobfuscate/Decode Files or Information

PipeMon can decrypt password-protected executables.[1]

Enterprise T1573 .001 Encrypted Channel: Symmetric Cryptography

PipeMon communications are RC4 encrypted.[1]

Enterprise T1008 Fallback Channels

PipeMon can switch to an alternate C2 domain when a particular date has been reached.[1]

Enterprise T1105 Ingress Tool Transfer

PipeMon can install additional modules via C2 commands.[1]

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

PipeMon modules are stored on disk with seemingly benign names including use of a file extension associated with a popular word processor.[1]

Enterprise T1112 Modify Registry

PipeMon has modified the Registry to store its encrypted payload.[1]

Enterprise T1106 Native API

PipeMon's first stage has been executed by a call to `CreateProcess` with the decryption password in an argument. PipeMon has used a call to `LoadLibrary` to load its installer.[1]

Enterprise T1095 Non-Application Layer Protocol

The PipeMon communication module can use a custom protocol based on TLS over TCP.[1]

Enterprise T1027 .011 Obfuscated Files or Information: Fileless Storage

PipeMon has stored its encrypted payload in the Registry under `HKLM\SOFTWARE\Microsoft\Print\Components\` .[1]

.013 Obfuscated Files or Information: Encrypted/Encoded File

PipeMon modules are stored encrypted on disk.[1]

Enterprise T1057 Process Discovery

PipeMon can iterate over the running processes to find a suitable injection target.[1]

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

PipeMon can inject its modules into various processes using reflective DLL loading.[1]

Enterprise T1129 Shared Modules

PipeMon has used call to `LoadLibrary` to load its installer. PipeMon loads its modules using reflective loading or custom shellcode.[1]

Enterprise T1518 .001 Software Discovery: Security Software Discovery

PipeMon can check for the presence of ESET and Kaspersky security software.[1]

Enterprise T1553 .002 Subvert Trust Controls: Code Signing

PipeMon, its installer, and tools are signed with stolen code-signing certificates.[1]

Enterprise T1082 System Information Discovery

PipeMon can collect and send OS version and computer name as a part of its C2 beacon.[1]

Enterprise T1016 System Network Configuration Discovery

PipeMon can collect and send the local IP address, RDP information, and the network adapter physical address as a part of its C2 beacon.[1]

Enterprise T1124 System Time Discovery

PipeMon can send time zone information from a compromised host to C2.[1]

---