

Misdat, Software S0083 | MITRE ATT&CK®

Archived: 2026-04-05 13:48:38 UTC

Enterprise [T1547 Boot or Logon Autostart Execution](#)

[Misdat](#) has created registry keys for persistence, including `HKCU\Software\dnimts0leht\StubPath` , `HKCU\Software\snimts0leht\StubPath` , `HKCU\Software\Backtsaleht\StubPath` , `HKLM\SOFTWARE\Microsoft\Active Setup\Installed. Components\{3bf41072-b2b1-21c8-b5c1-bd56d32fbda7}` , and `HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components\{3ef41072-a2f1-21c8-c5c1-70c2c3bc7905}` .^[1]

Enterprise [T1059 .003 Command and Scripting Interpreter: Windows Command Shell](#)

[Misdat](#) is capable of providing shell functionality to the attacker to execute commands.^[1]

Enterprise [T1132 .001 Data Encoding: Standard Encoding](#)

[Misdat](#) network traffic is Base64-encoded plaintext.^[1]

Enterprise [T1005 Data from Local System](#)

[Misdat](#) has collected files and data from a compromised host.^[1]

Enterprise [T1041 Exfiltration Over C2 Channel](#)

[Misdat](#) has uploaded files and data to its C2 servers.^[1]

Enterprise [T1083 File and Directory Discovery](#)

[Misdat](#) is capable of running commands to obtain a list of files and directories, as well as enumerating logical drives.^[1]

Enterprise [T1070 .004 Indicator Removal: File Deletion](#)

[Misdat](#) is capable of deleting the backdoor file.^[1]

[.006 Indicator Removal: Timestamp](#)

Many [Misdat](#) samples were programmed using Borland Delphi, which will mangle the default PE compile timestamp of a file.^[1]

[.009 Indicator Removal: Clear Persistence](#)

[Misdat](#) is capable of deleting Registry keys used for persistence.^[1]

Enterprise [T1105 Ingress Tool Transfer](#)

[Misdat](#) is capable of downloading files from the C2.^[1]

Enterprise [T1036 .005 Masquerading: Match Legitimate Resource Name or Location](#)

[Misdat](#) saves itself as a file named `msdtc.exe`, which is also the name of the legitimate Microsoft Distributed Transaction Coordinator service binary.^{[1][2]}

Enterprise [T1106 Native API](#)

[Misdat](#) has used Windows APIs, including `ExitWindowsEx` and `GetKeyboardType`.^[1]

Enterprise [T1095 Non-Application Layer Protocol](#)

[Misdat](#) network traffic communicates over a raw socket.^[1]

Enterprise [T1027 .002 Obfuscated Files or Information: Software Packing](#)

[Misdat](#) was typically packed using UPX.^[1]

Enterprise [T1082 System Information Discovery](#)

The initial beacon packet for [Misdat](#) contains the operating system version of the victim.^[1]

Enterprise [T1614 .001 System Location Discovery: System Language Discovery](#)

[Misdat](#) has attempted to detect if a compromised host had a Japanese keyboard via the Windows API call `GetKeyboardType`.^[1]

Source: <https://attack.mitre.org/software/S0083>