

MuddyWater, Earth Vetala, MERCURY, Static Kitten, Seedworm, TEMP.Zagros, Mango Sandstorm, TA450, Group G0069

Archived: 2026-04-05 15:59:57 UTC

Enterprise [T1548](#) [.002 Abuse Elevation Control Mechanism](#): [Bypass User Account Control](#)

[MuddyWater](#) uses various techniques to bypass UAC.^[4]

Enterprise [T1087](#) [.002 Account Discovery](#): [Domain Account](#)

[MuddyWater](#) has used `cmd.exe net user /domain` to enumerate domain users.^[9]

Enterprise [T1583](#) [.006 Acquire Infrastructure](#): [Web Services](#)

[MuddyWater](#) has used file sharing services including OneHub, Sync, and TeraBox to distribute tools.^{[10][9][13]}

Enterprise [T1071](#) [.001 Application Layer Protocol](#): [Web Protocols](#)

[MuddyWater](#) has used HTTP for C2 communications.^{[5][9]}

Enterprise [T1560](#) [.001 Archive Collected Data](#): [Archive via Utility](#)

[MuddyWater](#) has used the native Windows cabinet creation tool, makecab.exe, likely to compress stolen data to be uploaded.^[3]

Enterprise [T1547](#) [.001 Boot or Logon Autostart Execution](#): [Registry Run Keys / Startup Folder](#)

[MuddyWater](#) has added Registry Run key

`KCU\Software\Microsoft\Windows\CurrentVersion\Run\SystemTextEncoding` to establish persistence.^{[11][14][15][6][9][8]}

Enterprise [T1059](#) [.001 Command and Scripting Interpreter](#): [PowerShell](#)

[MuddyWater](#) has used PowerShell for execution.^{[11][16][14][3][4][15][6][9][7][8]}

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

[MuddyWater](#) has used a custom tool for creating reverse shells.^[3]

[.005 Command and Scripting Interpreter](#): [Visual Basic](#)

[MuddyWater](#) has used VBScript files to execute its [POWERSTATS](#) payload, as well as macros.^{[11][16][14][3][4][5][6][9][8]}

[.006 Command and Scripting Interpreter](#): [Python](#)

[MuddyWater](#) has developed tools in Python including [Out1](#).^[9]

[.007 Command and Scripting Interpreter: JavaScript](#)

[MuddyWater](#) has used JavaScript files to execute its [POWERSTATS](#) payload.^{[4][11][7]}

Enterprise [T1555 Credentials from Password Stores](#)

[MuddyWater](#) has performed credential dumping with [LaZagne](#) and other tools, including by dumping passwords saved in victim email.^{[2][3][9]}

[.003 Credentials from Web Browsers](#)

[MuddyWater](#) has run tools including Browser64 to steal passwords saved in victim web browsers.^{[3][9]}

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

[MuddyWater](#) has used tools to encode C2 communications including Base64 encoding.^{[5][9]}

Enterprise [T1074 .001 Data Staged: Local Data Staging](#)

[MuddyWater](#) has stored a decoy PDF file within a victim's `%temp%` folder.^[8]

Enterprise [T1140 Deobfuscate/Decode Files or Information](#)

[MuddyWater](#) has decoded base64-encoded PowerShell, JavaScript, and VBScript.^{[11][16][4][8]}

Enterprise [T1573 .001 Encrypted Channel: Symmetric Cryptography](#)

[MuddyWater](#) has used AES to encrypt C2 responses.^[8]

Enterprise [T1041 Exfiltration Over C2 Channel](#)

[MuddyWater](#) has used C2 infrastructure to receive exfiltrated data.^[6]

Enterprise [T1190 Exploit Public-Facing Application](#)

[MuddyWater](#) has exploited the Microsoft Exchange memory corruption vulnerability (CVE-2020-0688).^[7]

Enterprise [T1203 Exploitation for Client Execution](#)

[MuddyWater](#) has exploited the Office vulnerability CVE-2017-0199 for execution.^[5]

Enterprise [T1210 Exploitation of Remote Services](#)

[MuddyWater](#) has exploited the Microsoft Netlogon vulnerability (CVE-2020-1472).^[7]

Enterprise [T1083 File and Directory Discovery](#)

[MuddyWater](#) has used malware that checked if the ProgramData folder had folders or files with the keywords "Kasper," "Panda," or "ESET."^[14]

Enterprise [T1574 .001 Hijack Execution Flow: DLL](#)

[MuddyWater](#) maintains persistence on victim networks through side-loading dlls to trick legitimate programs into running malware.^[7]

Enterprise [T1562 .001 Impair Defenses: Disable or Modify Tools](#)

[MuddyWater](#) can disable the system's local proxy settings.^[9]

Enterprise [T1105 Ingress Tool Transfer](#)

[MuddyWater](#) has used malware that can upload additional files to the victim's machine.^{[14][4][6][9]}

Enterprise [T1559 .001 Inter-Process Communication: Component Object Model](#)

[MuddyWater](#) has used malware that has the capability to execute malicious code via COM, DCOM, and Outlook.^{[14][5][7]}

[.002 Inter-Process Communication: Dynamic Data Exchange](#)

[MuddyWater](#) has used malware that can execute PowerShell scripts via DDE.^[14]

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

[MuddyWater](#) has disguised malicious executables and used filenames and Registry key names associated with Windows Defender.^{[11][15][10]}

Enterprise [T1104 Multi-Stage Channels](#)

[MuddyWater](#) has used one C2 to obtain enumeration scripts and monitor web logs, but a different C2 to send data back.^[15]

Enterprise [T1027 .003 Obfuscated Files or Information: Steganography](#)

[MuddyWater](#) has stored obfuscated JavaScript code in an image file named temp.jpg.^[4]

[.004 Obfuscated Files or Information: Compile After Delivery](#)

[MuddyWater](#) has used the .NET csc.exe tool to compile executables from downloaded C# code.^[4]

[.010 Obfuscated Files or Information: Command Obfuscation](#)

[MuddyWater](#) has used Daniel Bohannon's Invoke-Obfuscation framework and obfuscated PowerShell scripts.^[2]

^[17] The group has also used other obfuscation methods, including Base64 obfuscation of VBScripts and PowerShell commands.^{[2][11][14][15][5][9][8]}

Enterprise [T1588 .002 Obtain Capabilities](#): [Tool](#)

[MuddyWater](#) has used legitimate tools [ConnectWise](#), [RemoteUtilities](#), and SimpleHelp to gain access to the target environment. [\[10\]\[18\]](#)

Enterprise [T1137 .001 Office Application Startup](#): [Office Template Macros](#)

[MuddyWater](#) has used a Word Template, Normal.dotm, for persistence. [\[6\]](#)

Enterprise [T1003 .001 OS Credential Dumping](#): [LSASS Memory](#)

[MuddyWater](#) has performed credential dumping with [Mimikatz](#) and procdump64.exe. [\[2\]\[3\]\[9\]](#)

[.004 OS Credential Dumping](#): [LSA Secrets](#)

[MuddyWater](#) has performed credential dumping with [LaZagne](#). [\[2\]\[3\]](#)

[.005 OS Credential Dumping](#): [Cached Domain Credentials](#)

[MuddyWater](#) has performed credential dumping with [LaZagne](#). [\[2\]\[3\]](#)

Enterprise [T1566 .001 Phishing](#): [Spearphishing Attachment](#)

[MuddyWater](#) has compromised third parties and used compromised accounts to send spearphishing emails with targeted attachments to recipients. [\[2\]\[11\]\[14\]\[5\]\[10\]\[9\]](#) [\[7\]\[13\]](#)

[.002 Phishing](#): [Spearphishing Link](#)

[MuddyWater](#) has sent targeted spearphishing e-mails with malicious links. [\[10\]\[9\]\[13\]](#)

Enterprise [T1057 Process Discovery](#)

[MuddyWater](#) has used malware to obtain a list of running processes on the system. [\[14\]\[5\]](#)

Enterprise [T1090 .002 Proxy](#): [External Proxy](#)

[MuddyWater](#) has controlled [POWERSTATS](#) from behind a proxy network to obfuscate the C2 location. [\[3\]](#)

[MuddyWater](#) has used a series of compromised websites that victims connected to randomly to relay information to command and control (C2). [\[6\]\[9\]](#)

Enterprise [T1219 Remote Access Tools](#)

[MuddyWater](#) has used legitimate applications ScreenConnect, AteraAgent and SimpleHelp to manage systems remotely and move laterally. [\[9\]\[10\]\[13\]\[18\]](#)

Enterprise [T1053 .005 Scheduled Task/Job](#): [Scheduled Task](#)

[MuddyWater](#) has used scheduled tasks to establish persistence. [\[6\]](#)

Enterprise [T1113 Screen Capture](#)

[MuddyWater](#) has used malware that can capture screenshots of the victim's machine. [\[14\]](#)

Enterprise [T1518 Software Discovery](#)

[MuddyWater](#) has used a PowerShell backdoor to check for Skype connectivity on the target machine. [\[9\]](#)

[.001 Security Software Discovery](#)

[MuddyWater](#) has used malware to check running processes against a hard-coded list of security tools often used by malware researchers. [\[14\]](#)

Enterprise [T1218 .003 System Binary Proxy Execution: CMSTP](#)

[MuddyWater](#) has used CMSTP.exe and a malicious INF to execute its [POWERSTATS](#) payload. [\[11\]](#)

[.005 System Binary Proxy Execution: Mshta](#)

[MuddyWater](#) has used mshta.exe to execute its [POWERSTATS](#) payload and to pass a PowerShell one-liner for execution. [\[11\]\[14\]](#)

[.011 System Binary Proxy Execution: Rundll32](#)

[MuddyWater](#) has used malware that leveraged rundll32.exe in a Registry Run key to execute a .dll. [\[14\]](#)

Enterprise [T1082 System Information Discovery](#)

[MuddyWater](#) has used malware that can collect the victim's OS version and machine name. [\[14\]\[15\]\[6\]\[9\]\[8\]](#)

Enterprise [T1016 System Network Configuration Discovery](#)

[MuddyWater](#) has used malware to collect the victim's IP address and domain name. [\[14\]](#)

Enterprise [T1049 System Network Connections Discovery](#)

[MuddyWater](#) has used a PowerShell backdoor to check for Skype connections on the target machine. [\[9\]](#)

Enterprise [T1033 System Owner/User Discovery](#)

[MuddyWater](#) has used malware that can collect the victim's username. [\[14\]\[9\]](#)

Enterprise [T1552 .001 Unsecured Credentials: Credentials In Files](#)

[MuddyWater](#) has run a tool that steals passwords saved in victim email. [\[3\]](#)

Enterprise [T1204 .001 User Execution: Malicious Link](#)

[MuddyWater](#) has distributed URLs in phishing e-mails that link to lure documents. [\[10\]\[9\]\[13\]](#)

[.002 User Execution: Malicious File](#)

[MuddyWater](#) has attempted to get users to open malicious PDF attachment and to enable macros and launch malicious Microsoft Word documents delivered via spearphishing emails. [\[2\]\[11\]\[14\]\[15\]\[5\]\[6\]\[10\]\[9\]\[7\]\[8\]\[13\]](#)

Enterprise [T1102 .002 Web Service: Bidirectional Communication](#)

[MuddyWater](#) has used web services including OneHub to distribute remote access tools. [\[10\]](#)

Enterprise [T1047 Windows Management Instrumentation](#)

[MuddyWater](#) has used malware that leveraged WMI for execution and querying host information. [\[14\]\[4\]\[15\]\[7\]](#)

Source: <https://attack.mitre.org/groups/G0069>