

FunnyDream, Software S1044 | MITRE ATT&CK®

Archived: 2026-04-05 13:57:31 UTC

Enterprise [T1010 Application Window Discovery](#)

[FunnyDream](#) has the ability to discover application windows via execution of `EnumWindows`.^[1]

Enterprise [T1560 .002 Archive Collected Data: Archive via Library](#)

[FunnyDream](#) has compressed collected files with zLib.^[1]

[.003 Archive Collected Data: Archive via Custom Method](#)

[FunnyDream](#) has compressed collected files with zLib and encrypted them using an XOR operation with the string key from the command line or `qwerasdf` if the command line argument doesn't contain the key. File names are obfuscated using XOR with the same key as the compressed file content.^[1]

Enterprise [T1119 Automated Collection](#)

[FunnyDream](#) can monitor files for changes and automatically collect them.^[1]

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

[FunnyDream](#) can use a Registry Run Key and the Startup folder to establish persistence.^[1]

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

[FunnyDream](#) can use `cmd.exe` for execution on remote hosts.^[1]

Enterprise [T1543 .003 Create or Modify System Process: Windows Service](#)

[FunnyDream](#) has established persistence by running `sc.exe` and by setting the `WSearch` service to run automatically.^[1]

Enterprise [T1005 Data from Local System](#)

[FunnyDream](#) can upload files from victims' machines.^{[1][2]}

Enterprise [T1025 Data from Removable Media](#)

The [FunnyDream](#) FilePakMonitor component has the ability to collect files from removable devices.^[1]

Enterprise [T1001 Data Obfuscation](#)

[FunnyDream](#) can send compressed and obfuscated packets to C2.^[1]

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

[FunnyDream](#) can stage collected information including screen captures and logged keystrokes locally.^[1]

Enterprise [T1041 Exfiltration Over C2 Channel](#)

[FunnyDream](#) can execute commands, including gathering user information, and send the results to C2.^[1]

Enterprise [T1083 File and Directory Discovery](#)

[FunnyDream](#) can identify files with .doc, .docx, .ppt, .pptx, .xls, .xlsx, and .pdf extensions and specific timestamps for collection.^[1]

Enterprise [T1070 Indicator Removal](#)

[FunnyDream](#) has the ability to clean traces of malware deployment.^[1]

[.004 File Deletion](#)

[FunnyDream](#) can delete files including its dropper component.^[1]

Enterprise [T1105 Ingress Tool Transfer](#)

[FunnyDream](#) can download additional files onto a compromised host.^[1]

Enterprise [T1056 .001 Input Capture: Keylogging](#)

The [FunnyDream](#) Keyrecord component can capture keystrokes.^[1]

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

[FunnyDream](#) can use com objects identified with `CLSID_ShellLink` (`IShellLink` and `IPersistFile`) and `WScript.Shell` (`RegWrite` method) to enable persistence mechanisms.^[1]

Enterprise [T1680 Local Storage Discovery](#)

[FunnyDream](#) can enumerate all logical drives on a targeted machine.^[1]

Enterprise [T1036 .004 Masquerading: Masquerade Task or Service](#)

[FunnyDream](#) has used a service named `WSearch` for execution.^[1]

Enterprise [T1106 Native API](#)

[FunnyDream](#) can use Native API for defense evasion, discovery, and collection.^[1]

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

[FunnyDream](#) can communicate with C2 over TCP and UDP.^[1]

Enterprise [T1027 .013 Obfuscated Files or Information: Encrypted/Encoded File](#)

[FunnyDream](#) can Base64 encode its C2 address stored in a template binary with the `xyz0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz_ -` or `xyz0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz_ =` character sets.^[1]

Enterprise [T1120 Peripheral Device Discovery](#)

The [FunnyDream](#) FilepakMonitor component can detect removable drive insertion.^[1]

Enterprise [T1057 Process Discovery](#)

[FunnyDream](#) has the ability to discover processes, including `Bka.exe` and `BkavUtil.exe`.^[1]

Enterprise [T1055 .001 Process Injection: Dynamic-link Library Injection](#)

The [FunnyDream](#) FilepakMonitor component can inject into the `Bka.exe` process using the `VirtualAllocEx`, `WriteProcessMemory` and `CreateRemoteThread` APIs to load the DLL component.^[1]

Enterprise [T1572 Protocol Tunneling](#)

[FunnyDream](#) can connect to HTTP proxies via TCP to create a tunnel to C2.^[1]

Enterprise [T1090 Proxy](#)

[FunnyDream](#) can identify and use configured proxies in a compromised network for C2 communication.^[1]

Enterprise [T1012 Query Registry](#)

[FunnyDream](#) can check `Software\Microsoft\Windows\CurrentVersion\Internet Settings` to extract the `ProxyServer` string.^[1]

Enterprise [T1018 Remote System Discovery](#)

[FunnyDream](#) can collect information about hosts on the victim network.^[2]

Enterprise [T1113 Screen Capture](#)

The [FunnyDream](#) ScreenCap component can take screenshots on a compromised host.^[1]

Enterprise [T1518 .001 Software Discovery: Security Software Discovery](#)

[FunnyDream](#) can identify the processes for Bkav antivirus.^[1]

Enterprise [T1218 .011 System Binary Proxy Execution: Rundll32](#)

[FunnyDream](#) can use `rundll32` for execution of its components.^[1]

Enterprise [T1016 System Network Configuration Discovery](#)

[FunnyDream](#) can parse the `ProxyServer` string in the Registry to discover http proxies. ^[1]

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

[FunnyDream](#) has the ability to gather user information from the targeted system using

```
whoami/upn&whoami/fqdn&whoami/logonid&whoami/all .[1]
```

Enterprise [T1124 System Time Discovery](#)

[FunnyDream](#) can check system time to help determine when changes were made to specified files. ^[1]

Enterprise [T1047 Windows Management Instrumentation](#)

[FunnyDream](#) can use WMI to open a Windows command shell on a remote machine. ^[1]

Source: <https://attack.mitre.org/software/S1044>