Bandook, Software S0234 | MITRE ATT&CK®

Archived: 2026-04-05 12:53:54 UTC

Enterprise T1123 Audio Capture

Bandook has modules that are capable of capturing audio.[1]

Enterprise T1059 Command and Scripting Interpreter

Bandook can support commands to execute Java-based payloads.[3]

.001 PowerShell

Bandook has used PowerShell loaders as part of execution.[3]

.003 Windows Command Shell

Bandook is capable of spawning a Windows command shell.[1][3]

.005 Visual Basic

Bandook has used malicious VBA code against the target system.[3]

.006 Python

Bandook can support commands to execute Python-based payloads.[3]

Enterprise T1005 Data from Local System

Bandook can collect local files from the system .[3]

Enterprise T1140 Deobfuscate/Decode Files or Information

Bandook has decoded its PowerShell script.[3]

Enterprise T1573 .001 Encrypted Channel: Symmetric Cryptography

Bandook has used AES encryption for C2 communication.[3]

Enterprise T1041 Exfiltration Over C2 Channel

Bandook can upload files from a victim's machine over the C2 channel.[3]

Enterprise T1083 File and Directory Discovery

Bandook has a command to list files on a system.[3]

Enterprise T1070 .004 Indicator Removal: File Deletion

Bandook has a command to delete a file.[3]

Enterprise T1105 Ingress Tool Transfer

Bandook can download files to the system.[3]

Enterprise T1056 .001 Input Capture: Keylogging

Bandook contains keylogging capabilities.[4]

Enterprise T1680 Local Storage Discovery

Bandook can collect information about the drives available on the system.[3]

Enterprise T1106 Native API

Bandook has used the ShellExecuteW() function call.[3]

Enterprise T1095 Non-Application Layer Protocol

Bandook has a command built in to use a raw TCP socket.[3]

Enterprise T1027 .003 Obfuscated Files or Information: Steganography

Bandook has used .PNG images within a zip file to build the executable. [3]

Enterprise T1120 Peripheral Device Discovery

Bandook can detect USB devices.[1]

Enterprise T1566 .001 Phishing: Spearphishing Attachment

Bandook is delivered via a malicious Word document inside a zip file.[3]

Enterprise T1055 .012 Process Injection: Process Hollowing

Bandook has been launched by starting iexplore.exe and replacing it with Bandook's payload.[2][1][3]

Enterprise T1113 Screen Capture

Bandook is capable of taking an image of and uploading the current desktop.[2][3]

Enterprise T1553 .002 Subvert Trust Controls: Code Signing

Bandook was signed with valid Certum certificates.[3]

Enterprise T1016 System Network Configuration Discovery

Bandook has a command to get the public IP address from a system.[3]

Enterprise T1204 .002 User Execution: Malicious File

Bandook has used lure documents to convince the user to enable macros.[3]

Enterprise T1125 Video Capture

Bandook has modules that are capable of capturing video from a victim's webcam.[1]
