BOOKWORM, Software S1226 | MITRE ATT&CK®

Archived: 2026-04-05 17:23:14 UTC

Enterprise T1071 .001 Application Layer Protocol: Web Protocols

BOOKWORM has communicated with its C2 via HTTP POST requests. [2][3]

Enterprise T1115 Clipboard Data

BOOKWORM has used its KBLogger.dll module to steal data saved to the clipboard. [2]

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

BOOKWORM has created a service named `Microsoft Windows DeviceSync Service` at `HKLM\SYSTEM\CurrentControlSet\Services\DeviceSync\` to trigger execution when the system starts and to maintain persistence. [2]

Enterprise T1001 .003 Data Obfuscation: Protocol or Service Impersonation

BOOKWORM has modified HTTP POST requests to resemble legitimate communications.[3]

Enterprise T1140 Deobfuscate/Decode Files or Information

BOOKWORM has decoded its Base64 encoded payload prior to execution.[3] BOOKWORM has also encrypted files with RC4 and has decrypted its payload prior to execution.[2]

Enterprise T1573 .001 Encrypted Channel: Symmetric Cryptography

BOOKWORM has used encryption and compression algorithms to obfuscate the traffic between the system and C2 server, methods observed included RC4, AES, XOR with 0x5a, and LZO. [2]

Enterprise T1564 .003 Hide Artifacts: Hidden Window

BOOKWORM has created a hidden window when conducting key logging and clipboard theft through its KBLogger.dll module.[2]

Enterprise T1574 .001 Hijack Execution Flow: DLL

BOOKWORM has used DLL side-loading to execute the malicious payload. [1][3] BOOKWORM has also side-loaded DLL components into a legitimate process, including Microsoft Malware Protection `MsMpEng.exe` and Kaspersky Anti-Virus `ushata.exe`.[2]

Enterprise T1070 .006 Indicator Removal: Timestomp

BOOKWORM has modified file timestamps from the export address table (EAT) to make it difficult to discern when the module was created. [3]

Enterprise T1056 .001 Input Capture: Keylogging

BOOKWORM has used its KBLogger.dll module to capture keystrokes and stored them in a folder. [2]

Enterprise T1036 .004 Masquerading: Masquerade Task or Service

BOOKWORM has created services that attempt to resemble legitimate services to include a service named `Microsoft Windows DeviceSync Service`.[2]

Enterprise T1112 Modify Registry

BOOKWORM has modified Registry key values as part of its created service `DeviceSync`. [2]

Enterprise T1106 Native API

BOOKWORM has used various Windows API calls during execution and defense evasion.[1] [3] BOOKWORM has created a buffer on the heap using `HeapCreate` and `HeapAlloc` which allows for copying of shell code and then execution on the heap is initiated through callback function of legitimate API functions such as `EnumChildWindows` or `EnumSystemLanguageGroupsA`. [3]

Enterprise T1027 Obfuscated Files or Information

BOOKWORM has been delivered using self-extracting RAR archives.[2]

.013 Encrypted/Encoded File

BOOKWORM has utilized Base64 encoding to obfuscate its payload.[3]

Enterprise T1553 .002 Subvert Trust Controls: Code Signing

BOOKWORM has used valid legitimate digital signatures and certificates to evade detection. [2]

Enterprise T1033 System Owner/User Discovery

BOOKWORM has obtained the username from an infected host. [2]
