# BendyBear, Software S0574 | MITRE ATT&CK®

Archived: 2026-04-05 13:07:40 UTC

| Domain | ID | | Name | Use |
|---|---|---|---|---|
| Enterprise | T1001 | .001 | Data Obfuscation: Junk Data | BendyBear has used byte randomization to obscure its behavior.[1] |
| Enterprise | T1140 | | Deobfuscate/Decode Files or Information | BendyBear has decrypted function blocks using a XOR key during runtime to evade detection.[1] |
| Enterprise | T1573 | .001 | Encrypted Channel: Symmetric Cryptography | BendyBear communicates to a C2 server over port 443 using modified RC4 and XOR-encrypted chunks.[1] |
| Enterprise | T1105 | | Ingress Tool Transfer | BendyBear is designed to download an implant from a C2 server.[1] |
| Enterprise | T1106 | | Native API | BendyBear can load and execute modules and Windows Application Programming (API) calls using standard shellcode API hashing.[1] |
| Enterprise | T1571 | | Non-Standard Port | BendyBear has used a custom RC4 and XOR encrypted protocol over port 443 for C2.[1] |
| Enterprise | T1027 | .013 | Obfuscated Files or Information: Encrypted/Encoded File | BendyBear has encrypted payloads using RC4 and XOR.[1] |
| | | .014 | Obfuscated Files or Information: Polymorphic Code | BendyBear changes its runtime footprint during code execution to evade signature-based defenses.[1] |

| Domain | ID | | Name | Use |
|---|---|---|---|---|
| Enterprise | T1012 | | Query Registry | BendyBear can query the host's Registry key at `HKEY_CURRENT_USER\Console\QuickEdit` to retrieve data.[1] |
| Enterprise | T1124 | | System Time Discovery | BendyBear has the ability to determine local time on a compromised host.[1] |
| Enterprise | T1497 | .003 | Virtualization/Sandbox Evasion: Time Based Checks | BendyBear can check for analysis environments and signs of debugging using the Windows API `kernel32!GetTickCountKernel32` call.[1] |

---

Source: https://attack.mitre.org/software/S0574