# Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:39:01 UTC



## Tool: ZIPLINE

| | |
|---|---|
| Names | ZIPLINE |
| Category | Malware |
| Type | Backdoor |
| Description | (Mandiant) ZIPLINE is a passive backdoor that hijacks an exported function, accept(), from the file libsecure.so. When ZIPLINE invokes the hijacked accept() function, it first resolves the benign accept() from libc, to intercept network traffic. Once an incoming connection is registered, it is first processed by the benign libc_accept, and ZIPLINE then checks if the process name is “web”. The malware retrieves up to 21 bytes from the connected host, verifying if the received buffer corresponds to the string “SSH-2.0-OpenSSH_0.3xx.” If so, the malicious functionality of ZIPLINE is triggered. ZIPLINE will then receive an encrypted header which specifies the command to be executed. Further details about this hijacking technique for the accept() function can be found in this SecureIdeas post. |
| Information | <https://www.mandiant.com/resources/blog/suspected-apt-targets-ivanti-zero-day> |
| MITRE ATT&CK | <https://attack.mitre.org/software/S1114> |

Last change to this tool card: 19 June 2024

Download this tool card in JSON format

### All groups using tool ZIPLINE

| Changed | Name | Country | Observed | |
|---|---|---|---|---|
| **APT groups** | | | | |
| | UNC5221, UTA0178 | | 2022-Mar 2025 | |

*1 group listed (1 APT, 0 other, 0 unknown)*

---