

## Octopus, Software S0340 | MITRE ATT&CK®

Archived: 2026-04-02 12:03:43 UTC

Enterprise [T1071 .001 Application Layer Protocol](#): [Web Protocols](#)

[Octopus](#) has used HTTP GET and POST requests for C2 communications. [\[1\]](#)[\[3\]](#)

Enterprise [T1560 .001 Archive Collected Data](#): [Archive via Utility](#)

[Octopus](#) has compressed data before exfiltrating it using a tool called Abbrevia. [\[3\]](#)

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

[Octopus](#) achieved persistence by placing a malicious executable in the startup directory and has added the `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run` key to the Registry. [\[1\]](#)

Enterprise [T1132 .001 Data Encoding](#): [Standard Encoding](#)

[Octopus](#) has encoded C2 communications in Base64. [\[1\]](#)

Enterprise [T1005 Data from Local System](#)

[Octopus](#) can exfiltrate files from the system using a documents collector tool. [\[3\]](#)

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

[Octopus](#) has stored collected information in the Application Data directory on a compromised host. [\[1\]](#)[\[3\]](#)

Enterprise [T1041 Exfiltration Over C2 Channel](#)

[Octopus](#) has uploaded stolen files and data from a victim's machine over its C2 channel. [\[1\]](#)

Enterprise [T1567 .002 Exfiltration Over Web Service](#): [Exfiltration to Cloud Storage](#)

[Octopus](#) has exfiltrated data to file sharing sites. [\[3\]](#)

Enterprise [T1083 File and Directory Discovery](#)

[Octopus](#) can collect information on the Windows directory and searches for compressed RAR files on the host. [\[1\]](#)[\[2\]](#)[\[3\]](#)

Enterprise [T1105 Ingress Tool Transfer](#)

[Octopus](#) can download additional files and tools onto the victim's machine. [\[1\]](#)[\[2\]](#)[\[3\]](#)

Enterprise [T1680 Local Storage Discovery](#)

[Octopus](#) can collect system drive and disk size information.<sup>[1]</sup>

Enterprise [T1036 .005 Masquerading: Match Legitimate Resource Name or Location](#)

[Octopus](#) has been disguised as legitimate programs, such as Java and Telegram Messenger.<sup>[1][3]</sup>

Enterprise [T1566 .001 Phishing: Spearphishing Attachment](#)

[Octopus](#) has been delivered via spearsphishing emails.<sup>[3]</sup>

Enterprise [T1113 Screen Capture](#)

[Octopus](#) can capture screenshots of the victims' machine.<sup>[1][2][3]</sup>

Enterprise [T1082 System Information Discovery](#)

[Octopus](#) can collect the computer name, OS version, and OS architecture information.<sup>[1]</sup>

Enterprise [T1016 System Network Configuration Discovery](#)

[Octopus](#) can collect the host IP address from the victim's machine.<sup>[1]</sup>

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

[Octopus](#) can collect the username from the victim's machine.<sup>[1]</sup>

Enterprise [T1204 .002 User Execution: Malicious File](#)

[Octopus](#) has relied upon users clicking on a malicious attachment delivered through spearphishing.<sup>[3]</sup>

Enterprise [T1047 Windows Management Instrumentation](#)

[Octopus](#) has used wmic.exe for local discovery information.<sup>[1]</sup>

---

Source: <https://attack.mitre.org/software/S0340/>