Drovorub, Software S0502 | MITRE ATT&CK®

Archived: 2026-04-05 14:51:53 UTC

Domain	ID		Name	Use
Enterprise	T1071	.001	Application Layer Protocol: Web Protocols	Drovorub can use the WebSocket protocol and has initiated communication with C2 servers with an HTTP Upgrade request.[1]
Enterprise	T1547	.006	Boot or Logon Autostart Execution: Kernel Modules and Extensions	Drovorub can use kernel modules to establish persistence.[1]
Enterprise	T1059	.004	Command and Scripting Interpreter: Unix Shell	Drovorub can execute arbitrary commands as root on a compromised system.[1]
Enterprise	T1005		Data from Local System	Drovorub can transfer files from the victim machine.[1]
Enterprise	T1140		Deobfuscate/Decode Files or Information	Drovorub has de-obsfuscated XOR encrypted payloads in WebSocket messages.[1]
Enterprise	T1041		Exfiltration Over C2 Channel	Drovorub can exfiltrate files over C2 infrastructure.[1]
Enterprise	T1070	.004	Indicator Removal: File Deletion	Drovorub can delete specific files from a compromised host.[1]
Enterprise	T1105		Ingress Tool Transfer	Drovorub can download files to a compromised host.[1]

Domain	ID		Name	Use
Enterprise	T1095		Non-Application Layer Protocol	Drovorub can use TCP to communicate between its agent and client modules.[1]
Enterprise	T1027		Obfuscated Files or Information	Drovorub has used XOR encrypted payloads in WebSocket client to server messages.[1]
Enterprise	T1090	.001	Proxy: Internal Proxy	Drovorub can use a port forwarding rule on its agent module to relay network traffic through the client module to a remote host on the same network.[1]
Enterprise	T1014		Rootkit	Drovorub has used a kernel module rootkit to hide processes, files, executables, and network artifacts from user space view.[1]

Source: https://attack.mitre.org/software/S0502