DEADWOOD, Software S1134 | MITRE ATT&CK®

Archived: 2026-04-05 18:20:22 UTC

Domain	ID		Name	Use
Enterprise	T1531		Account Access Removal	DEADWOOD changes the password for local and domain users via `net.exe` to a random 32 character string to prevent these accounts from logging on. Additionally, DEADWOOD will terminate the `winlogon.exe` process to prevent attempts to log on to the infected system.[1]
Enterprise	T1485		Data Destruction	DEADWOOD overwrites files on victim systems with random data to effectively destroy them.[1]
Enterprise	T1140		Deobfuscate/Decode Files or Information	DEADWOOD XORs some strings within the binary using the value `0xD5`, and deobfuscates these items at runtime.[1]
Enterprise	T1561	.001	Disk Wipe: Disk Content Wipe	DEADWOOD deletes files following overwriting them with random data.[1]
		.002	Disk Wipe: Disk Structure Wipe	DEADWOOD opens and writes zeroes to the first 512 bytes of each drive, deleting the MBR. DEADWOOD then sends the control code `IOCTL_DISK_DELETE_DRIVE_LAYOUT` to ensure the MBR is removed from the drive.[1]
Enterprise	T1036	.004	Masquerading: Masquerade Task or Service	DEADWOOD will attempt to masquerade its service execution using benign-looking names such as `ScDeviceEnums`.[1]
Enterprise	T1027	.009	Obfuscated Files or Information:	DEADWOOD contains an embedded, AES-encrypted payload labeled `METADATA` that

Domain	ID		Name	Use
			Embedded Payloads	provides configuration information for follow-on execution.[1]
		.013	Obfuscated Files or Information: Encrypted/Encoded File	DEADWOOD contains an embedded, AES-encrypted resource named `METADATA` that contains configuration information for follow-on execution.[1]
Enterprise	T1569	.002	System Services: Service Execution	DEADWOOD can be executed as a service using various names, such as `ScDeviceEnums`.[1]
Enterprise	T1124		System Time Discovery	DEADWOOD will set a timestamp value to determine when wiping functionality starts. When the timestamp is met on the system, a trigger file is created on the operating system allowing for execution to proceed. If the timestamp is in the past, the wiper will execute immediately.[1]

Source: https://attack.mitre.org/software/S1134