WindTail, Software S0466 | MITRE ATT&CK®

Archived: 2026-04-05 18:32:12 UTC

Domain	ID		Name	Use
Enterprise	T1071	.001	Application Layer Protocol: Web Protocols	WindTail has the ability to use HTTP for C2 communications.[3]
Enterprise	T1560	.001	Archive Collected Data: Archive via Utility	WindTail has the ability to use the macOS built-in zip utility to archive files.[3]
Enterprise	T1119		Automated Collection	WindTail can identify and add files that possess specific file extensions to an array for archiving.[3]
Enterprise	T1059	.004	Command and Scripting Interpreter: Unix Shell	WindTail can use the `open` command to execute an application.[2]
Enterprise	T1140		Deobfuscate/Decode Files or Information	WindTail has the ability to decrypt strings using hard-coded AES keys.[2]
Enterprise	T1048	.003	Exfiltration Over Alternative Protocol: Exfiltration Over Unencrypted Non-C2 Protocol	WindTail has the ability to automatically exfiltrate files using the macOS built-in utility /usr/bin/curl.[3]
Enterprise	T1083		File and Directory Discovery	WindTail has the ability to enumerate the users home directory and the path to its own application bundle.[2][3]
Enterprise	T1564	.003	Hide Artifacts: Hidden Window	WindTail can instruct the OS to execute an application without a dock icon or menu.[2]

Domain	ID		Name	Use
Enterprise	T1070	.004	Indicator Removal: File Deletion	WindTail has the ability to receive and execute a self-delete command.[3]
Enterprise	T1036		Masquerading	WindTail has used icons mimicking MS Office files to mask payloads.[2]
		.001	Invalid Code Signature	WindTail has been incompletely signed with revoked certificates.[2]
Enterprise	T1106		Native API	WindTail can invoke Apple APIs `contentsOfDirectoryAtPath`, `pathExtension`, and (string) `compare`.[3]
Enterprise	T1027	.013	Obfuscated Files or Information: Encrypted/Encoded File	WindTail can be delivered as a compressed, encrypted, and encoded payload.[3]
		.015	Obfuscated Files or Information: Compression	WindTail can be delivered as a compressed, encrypted, and encoded payload.[3]
Enterprise	T1124		System Time Discovery	WindTail has the ability to generate the current date and time.[2]

Source: https://attack.mitre.org/software/S0466/