TAINTEDSCRIBE, Software S0586 | MITRE ATT&CK®

Archived: 2026-04-05 18:27:20 UTC

Domain	ID		Name	Use
Enterprise	T1560		Archive Collected Data	TAINTEDSCRIBE has used `FileReadZipSend` to compress a file and send to C2.[1]
Enterprise	T1547	.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	TAINTEDSCRIBE can copy itself into the current user's Startup folder as "Narrator.exe" for persistence.[1]
Enterprise	T1059	.003	Command and Scripting Interpreter: Windows Command Shell	TAINTEDSCRIBE can enable Windows CLI access and execute files.[1]
Enterprise	T1001	.003	Data Obfuscation: Protocol or Service Impersonation	TAINTEDSCRIBE has used FakeTLS for session authentication.[1]
Enterprise	T1573	.001	Encrypted Channel: Symmetric Cryptography	TAINTEDSCRIBE uses a Linear Feedback Shift Register (LFSR) algorithm for network encryption.[1]
Enterprise	T1008		Fallback Channels	TAINTEDSCRIBE can randomly pick one of five hard-coded IP addresses for C2 communication; if one of the IP fails, it will wait 60 seconds and then try another IP address.[1]
Enterprise	T1083		File and Directory Discovery	TAINTEDSCRIBE can use `DirectoryList` to enumerate files in a specified directory.[1]
Enterprise	T1070	.004	Indicator Removal: File Deletion	TAINTEDSCRIBE can delete files from a compromised host.[1]

Domain	ID		Name	Use
		.006	Indicator Removal: Timestomp	TAINTEDSCRIBE can change the timestamp of specified filenames.[1]
Enterprise	T1105		Ingress Tool Transfer	TAINTEDSCRIBE can download additional modules from its C2 server.[1]
Enterprise	T1680		Local Storage Discovery	TAINTEDSCRIBE can use `DriveList` to retrieve drive information.[1]
Enterprise	T1036	.005	Masquerading: Match Legitimate Resource Name or Location	The TAINTEDSCRIBE main executable has disguised itself as Microsoft's Narrator.[1]
Enterprise	T1027	.001	Obfuscated Files or Information: Binary Padding	TAINTEDSCRIBE can execute `FileRecvWriteRand` to append random bytes to the end of a file received from C2.[1]
Enterprise	T1057		Process Discovery	TAINTEDSCRIBE can execute `ProcessList` for process discovery.[1]
Enterprise	T1018		Remote System Discovery	The TAINTEDSCRIBE command and execution module can perform target system enumeration.[1]
Enterprise	T1124		System Time Discovery	TAINTEDSCRIBE can execute `GetLocalTime` for time discovery.[1]