PUNCHBUGGY, Software S0196 | MITRE ATT&CK®

Archived: 2026-04-05 15:54:09 UTC

Domain	ID		Name	Use
Enterprise	T1087	.001	Account Discovery: Local Account	PUNCHBUGGY can gather user names.[1]
Enterprise	T1071	.001	Application Layer Protocol: Web Protocols	PUNCHBUGGY enables remote interaction and can obtain additional code over HTTPS GET and POST requests.[2][3] [1]
Enterprise	T1560	.001	Archive Collected Data: Archive via Utility	PUNCHBUGGY has Gzipped information and saved it to a random temp file before exfil.[1]
Enterprise	T1547	.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	PUNCHBUGGY has been observed using a Registry Run key.[3][1]
Enterprise	T1059	.001	Command and Scripting Interpreter: PowerShell	PUNCHBUGGY has used PowerShell scripts.[1]
		.006	Command and Scripting Interpreter: Python	PUNCHBUGGY has used python scripts. [1]
Enterprise	T1074	.001	Data Staged: Local Data Staging	PUNCHBUGGY has saved information to a random temp file before exfil.[1]
Enterprise	T1140		Deobfuscate/Decode Files or Information	PUNCHBUGGY has used PowerShell to decode base64-encoded assembly.[1]

Domain	ID		Name	Use
Enterprise	T1546	.009	Event Triggered Execution: AppCert DLLs	PUNCHBUGGY can establish using a AppCertDLLs Registry key.[3]
Enterprise	T1070	.004	Indicator Removal: File Deletion	PUNCHBUGGY can delete files written to disk.[3][1]
Enterprise	T1105		Ingress Tool Transfer	PUNCHBUGGY can download additional files and payloads to compromised hosts.[3] [1]
Enterprise	T1036	.005	Masquerading: Match Legitimate Resource Name or Location	PUNCHBUGGY mimics filenames from %SYSTEM%\System32 to hide DLLs in %WINDIR% and/or %TEMP%.[3][1]
Enterprise	T1027		Obfuscated Files or Information	PUNCHBUGGY has hashed most its code's functions and encrypted payloads with base64 and XOR.[1]
Enterprise	T1129		Shared Modules	PUNCHBUGGY can load a DLL using the LoadLibrary API.[3]
Enterprise	T1518	.001	Software Discovery: Security Software Discovery	PUNCHBUGGY can gather AVs registered in the system.[1]
Enterprise	T1218	.011	System Binary Proxy Execution: Rundll32	PUNCHBUGGY can load a DLL using Rundll32.[3]
Enterprise	T1082		System Information Discovery	PUNCHBUGGY can gather system information such as computer names.[1]

Source: https://attack.mitre.org/software/S0196/