Pony, Software S0453 | MITRE ATT&CK®

Archived: 2026-04-05 14:06:06 UTC

Domain	ID		Name	Use
Enterprise	T1087	.001	Account Discovery: Local Account	Pony has used the `NetUserEnum` function to enumerate local accounts.[1]
Enterprise	T1071	.001	Application Layer Protocol: Web Protocols	Pony has sent collected information to the C2 via HTTP POST request.[1]
Enterprise	T1110	.001	Brute Force: Password Guessing	Pony has used a small dictionary of common passwords against a collected list of local accounts.[1]
Enterprise	T1059	.003	Command and Scripting Interpreter: Windows Command Shell	Pony has used batch scripts to delete itself after execution.[1]
Enterprise	T1070	.004	Indicator Removal: File Deletion	Pony has used scripts to delete itself after execution.[1]
Enterprise	T1105		Ingress Tool Transfer	Pony can download additional files onto the infected system.[1]
Enterprise	T1036		Masquerading	Pony has used the Adobe Reader icon for the downloaded file to look more trustworthy.[1]
Enterprise	T1106		Native API	Pony has used several Windows functions for various purposes.[1]

Domain	ID		Name	Use
Enterprise	T1027	.015	Obfuscated Files or Information: Compression	Pony attachments have been delivered via compressed archive files.[1]
		.016	Obfuscated Files or Information: Junk Code Insertion	Pony obfuscates memory flow by adding junk instructions when executing to make analysis more difficult.[1]
Enterprise	T1566	.001	Phishing: Spearphishing Attachment	Pony has been delivered via spearphishing attachments.[1]
		.002	Phishing: Spearphishing Link	Pony has been delivered via spearphishing emails which contained malicious links.[1]
Enterprise	T1082		System Information Discovery	Pony has collected the Service Pack, language, and region information to send to the C2.[1]
Enterprise	T1204	.001	User Execution: Malicious Link	Pony has attempted to lure targets into clicking links in spoofed emails from legitimate banks.[1]
		.002	User Execution: Malicious File	Pony has attempted to lure targets into downloading an attached executable (ZIP, RAR, or CAB archives) or document (PDF or other MS Office format).[1]
Enterprise	T1497	.003	Virtualization/Sandbox Evasion: Time Based Checks	Pony has delayed execution using a built-in function to avoid detection and analysis.[1]