Xbash, Software S0341 | MITRE ATT&CK®

Archived: 2026-04-05 17:57:10 UTC

Domain	ID		Name	Use
Enterprise	T1071	.001	Application Layer Protocol: Web Protocols	Xbash uses HTTP for C2 communications.[1]
Enterprise	T1547	.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	Xbash can create a Startup item for persistence if it determines it is on a Windows system.[1]
Enterprise	T1110	.001	Brute Force: Password Guessing	Xbash can obtain a list of weak passwords from the C2 server to use for brute forcing as well as attempt to brute force services with open ports.[1][2]
Enterprise	T1059	.001	Command and Scripting Interpreter: PowerShell	Xbash can use scripts to invoke PowerShell to download a malicious PE executable or PE DLL for execution.[1]
		.005	Command and Scripting Interpreter: Visual Basic	Xbash can execute malicious VBScript payloads on the victim’s machine.[1]
		.007	Command and Scripting Interpreter: JavaScript	Xbash can execute malicious JavaScript payloads on the victim’s machine.[1]
Enterprise	T1485		Data Destruction	Xbash has destroyed Linux-based databases as part of its ransomware capabilities.[1]
Enterprise	T1486		Data Encrypted for Impact	Xbash has maliciously encrypted victim's database systems and demanded a cryptocurrency ransom be paid.[1]

Domain	ID		Name	Use
Enterprise	T1203		Exploitation for Client Execution	Xbash can attempt to exploit known vulnerabilities in Hadoop, Redis, or ActiveMQ when it finds those services running in order to conduct further execution.[1][2]
Enterprise	T1105		Ingress Tool Transfer	Xbash can download additional malicious files from its C2 server.[1]
Enterprise	T1046		Network Service Discovery	Xbash can perform port scanning of TCP and UDP ports.[1]
Enterprise	T1053	.003	Scheduled Task/Job: Cron	Xbash can create a cronjob for persistence if it determines it is on a Linux system.[1]
Enterprise	T1218	.005	System Binary Proxy Execution: Mshta	Xbash can use mshta for executing scripts.[1]
		.010	System Binary Proxy Execution: Regsvr32	Xbash can use regsvr32 for executing scripts.[1]
Enterprise	T1016		System Network Configuration Discovery	Xbash can collect IP addresses and local intranet information from a victim’s machine.[1]
Enterprise	T1102	.001	Web Service: Dead Drop Resolver	Xbash can obtain a webpage hosted on Pastebin to update its C2 domain list.[1]