Ixeshe, Software S0015 | MITRE ATT&CK®

Archived: 2026-04-02 11:03:21 UTC

Domain	ID		Name	Use
Enterprise	T1071	.001	Application Layer Protocol: Web Protocols	Ixeshe uses HTTP for command and control.[1][2]
Enterprise	T1547	.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	Ixeshe can achieve persistence by adding itself to the `HKCU\Software\Microsoft\Windows\CurrentVersion\Run` Registry key.[2]
Enterprise	T1059	.003	Command and Scripting Interpreter: Windows Command Shell	Ixeshe is capable of executing commands via cmd.[2]
Enterprise	T1132	.001	Data Encoding: Standard Encoding	Ixeshe uses custom Base64 encoding schemes to obfuscate command and control traffic in the message body of HTTP requests.[1][2]
Enterprise	T1005		Data from Local System	Ixeshe can collect data from a local system.[2]
Enterprise	T1083		File and Directory Discovery	Ixeshe can list file and directory information.[2]
Enterprise	T1564	.001	Hide Artifacts: Hidden Files and Directories	Ixeshe sets its own executable file's attributes to hidden.[2]

Domain	ID		Name	Use
Enterprise	T1070	.004	Indicator Removal: File Deletion	Ixeshe has a command to delete a file from the machine.[2]
Enterprise	T1105		Ingress Tool Transfer	Ixeshe can download and execute additional files.[2]
Enterprise	T1036	.005	Masquerading: Match Legitimate Resource Name or Location	Ixeshe has used registry values and file names associated with Adobe software, such as AcroRd32.exe.[2]
Enterprise	T1057		Process Discovery	Ixeshe can list running processes.[2]
Enterprise	T1082		System Information Discovery	Ixeshe collects the computer name of the victim's system during the initial infection.[2]
Enterprise	T1016		System Network Configuration Discovery	Ixeshe enumerates the IP address, network proxy settings, and domain name from a victim's system.[2]
Enterprise	T1033		System Owner/User Discovery	Ixeshe collects the username from the victim’s machine.[2]
Enterprise	T1007		System Service Discovery	Ixeshe can list running services.[2]