Action RAT, Software S1028 | MITRE ATT&CK®

Archived: 2026-04-05 15:11:20 UTC

Domain	ID		Name	Use
Enterprise	T1071	.001	Application Layer Protocol: Web Protocols	Action RAT can use HTTP to communicate with C2 servers.[1]
Enterprise	T1059	.003	Command and Scripting Interpreter: Windows Command Shell	Action RAT can use `cmd.exe` to execute commands on an infected host.[1]
Enterprise	T1005		Data from Local System	Action RAT can collect local data from an infected machine.[1]
Enterprise	T1140		Deobfuscate/Decode Files or Information	Action RAT can use Base64 to decode actor-controlled C2 server communications.[1]
Enterprise	T1083		File and Directory Discovery	Action RAT has the ability to collect drive and file information on an infected machine.[1]
Enterprise	T1105		Ingress Tool Transfer	Action RAT has the ability to download additional payloads onto an infected machine.[1]
Enterprise	T1027		Obfuscated Files or Information	Action RAT's commands, strings, and domains can be Base64 encoded within the payload.[1]

Domain	ID		Name	Use
Enterprise	T1518	.001	Software Discovery: Security Software Discovery	Action RAT can identify AV products on an infected host using the following command: `cmd.exe WMIC /Node:localhost /Namespace:\\root\SecurityCenter2 Path AntiVirusProduct Get displayName /Format:List` .[1]
Enterprise	T1082		System Information Discovery	Action RAT has the ability to collect the hostname, OS version, and OS architecture of an infected host.[1]
Enterprise	T1016		System Network Configuration Discovery	Action RAT has the ability to collect the MAC address of an infected host.[1]
Enterprise	T1033		System Owner/User Discovery	Action RAT has the ability to collect the username from an infected host.[1]
Enterprise	T1047		Windows Management Instrumentation	Action RAT can use WMI to gather AV products installed on an infected host.[1]
