Avenger, Software S0473 | MITRE ATT&CK®

Archived: 2026-04-05 15:29:14 UTC

Domain	ID		Name	Use
Enterprise	T1071	.001	Application Layer Protocol: Web Protocols	Avenger has the ability to use HTTP in communication with C2.[1]
Enterprise	T1140		Deobfuscate/Decode Files or Information	Avenger has the ability to decrypt files downloaded from C2.[1]
Enterprise	T1083		File and Directory Discovery	Avenger has the ability to browse files in directories such as Program Files and the Desktop.[1]
Enterprise	T1105		Ingress Tool Transfer	Avenger has the ability to download files from C2 to a compromised host.[1]
Enterprise	T1680		Local Storage Discovery	Avenger has the ability to identify the host volume ID.[1]
Enterprise	T1027	.003	Obfuscated Files or Information: Steganography	Avenger can extract backdoor malware from downloaded images.[1]
		.013	Obfuscated Files or Information: Encrypted/Encoded File	Avenger has the ability to XOR encrypt files to be sent to C2.[1]
Enterprise	T1057		Process Discovery	Avenger has the ability to use Tasklist to identify running processes.[1]

Domain	ID		Name	Use
Enterprise	T1055		Process Injection	Avenger has the ability to inject shellcode into svchost.exe.[1]
Enterprise	T1518	.001	Software Discovery: Security Software Discovery	Avenger has the ability to identify installed anti-virus products on a compromised host.[1]
Enterprise	T1082		System Information Discovery	Avenger has the ability to identify the OS architecture on a compromised host.[1]
Enterprise	T1016		System Network Configuration Discovery	Avenger can identify the domain of the compromised host.[1]

Source: https://attack.mitre.org/software/S0473