HiddenWasp, Software S0394 | MITRE ATT&CK®

Archived: 2026-04-05 13:49:29 UTC

Domain	ID		Name	Use
Enterprise	T1037	.004	Boot or Logon Initialization Scripts: RC Scripts	HiddenWasp installs reboot persistence by adding itself to `/etc/rc.local`.[1]
Enterprise	T1059	.003	Command and Scripting Interpreter: Windows Command Shell	HiddenWasp uses a script to automate tasks on the victim's machine and to assist in execution.[1]
Enterprise	T1136	.001	Create Account: Local Account	HiddenWasp creates a user account as a means to provide initial persistence to the compromised machine.[1]
Enterprise	T1140		Deobfuscate/Decode Files or Information	HiddenWasp uses a cipher to implement a decoding function.[1]
Enterprise	T1573	.001	Encrypted Channel: Symmetric Cryptography	HiddenWasp uses an RC4-like algorithm with an already computed PRGA generated key-stream for network communication.[1]
Enterprise	T1574	.006	Hijack Execution Flow: Dynamic Linker Hijacking	HiddenWasp adds itself as a shared object to the LD_PRELOAD environment variable.[1]
Enterprise	T1105		Ingress Tool Transfer	HiddenWasp downloads a tar compressed archive from a download server to the system.[1]

Domain	ID		Name	Use
Enterprise	T1095		Non-Application Layer Protocol	HiddenWasp communicates with a simple network protocol over TCP.[1]
Enterprise	T1027	.013	Obfuscated Files or Information: Encrypted/Encoded File	HiddenWasp encrypts its configuration and payload.[1]
Enterprise	T1014		Rootkit	HiddenWasp uses a rootkit to hook and implement functions on the system.[1]

Source: https://attack.mitre.org/software/S0394