GreyEnergy, Software S0342 | MITRE ATT&CK®

Archived: 2026-04-05 12:50:17 UTC

Domain	ID		Name	Use
Enterprise	T1071	.001	Application Layer Protocol: Web Protocols	GreyEnergy uses HTTP and HTTPS for C2 communications.[1]
Enterprise	T1059	.003	Command and Scripting Interpreter: Windows Command Shell	GreyEnergy uses cmd.exe to execute itself in-memory.[1]
Enterprise	T1543	.003	Create or Modify System Process: Windows Service	GreyEnergy chooses a service, drops a DLL file, and writes it to that serviceDLL Registry key.[1]
Enterprise	T1573	.001	Encrypted Channel: Symmetric Cryptography	GreyEnergy encrypts communications using AES256.[1]
		.002	Encrypted Channel: Asymmetric Cryptography	GreyEnergy encrypts communications using RSA-2048.[1]
Enterprise	T1070	.004	Indicator Removal: File Deletion	GreyEnergy can securely delete a file by hooking into the DeleteFileA and DeleteFileW functions in the Windows API.[1]
Enterprise	T1105		Ingress Tool Transfer	GreyEnergy can download additional modules and payloads.[1]
Enterprise	T1056	.001	Input Capture: Keylogging	GreyEnergy has a module to harvest pressed keystrokes.[1]

Domain	ID		Name	Use
Enterprise	T1112		Modify Registry	GreyEnergy modifies conditions in the Registry and adds keys.[1]
Enterprise	T1027	.002	Obfuscated Files or Information: Software Packing	GreyEnergy is packed for obfuscation.[1]
		.013	Obfuscated Files or Information: Encrypted/Encoded File	GreyEnergy encrypts its configuration files with AES-256 and also encrypts its strings.[1]
Enterprise	T1003	.001	OS Credential Dumping: LSASS Memory	GreyEnergy has a module for Mimikatz to collect Windows credentials from the victim's machine.[1]
Enterprise	T1055	.002	Process Injection: Portable Executable Injection	GreyEnergy has a module to inject a PE binary into a remote process.[1]
Enterprise	T1090	.003	Proxy: Multi-hop Proxy	GreyEnergy has used Tor relays for Command and Control servers.[1]
Enterprise	T1553	.002	Subvert Trust Controls: Code Signing	GreyEnergy digitally signs the malware with a code-signing certificate.[1]
Enterprise	T1218	.011	System Binary Proxy Execution: Rundll32	GreyEnergy uses PsExec locally in order to execute rundll32.exe at the highest privileges (NTAUTHORITY\SYSTEM).[1]
Enterprise	T1007		System Service Discovery	GreyEnergy enumerates all Windows services.[1]